Cellebrite
UFED

Touch Overview guide

May 2021 | Version 7.45

Cellebrite

Legal notices

Warnings

WARNING: Cellebrite UFED Touch should be used only with the dedicated AC/DC adapter supplied with this device.

WARNING: USB, Ethernet and target and source connectors should be connected only to CE approved devices (according to IEC/EN 60065 standard).

WARNING: Make sure that all external connections to other devices (except for the power adapter) are only indoor and SELV (safety extra low voltage, not exceed 42.4 V peak or 60 VDC).

FCC WARNING: This device complies with part 15 of the FCC rules. Operation is subject to the following two conditions:

1) This device may not cause harmful interference.

2) This device must accept any interference received, including interference that may cause undesired operation.

BATTERY WARNING: There is a danger of explosion if the battery is replaced incorrectly. Replace only with the same or equivalent type recommended by the manufacturer. Before disposing the battery, make sure it is fully discharged. Discard used batteries according to regulation in your country.

Contents

Cellebrite

1. Introduction

Cellebrite UFED Touch is a new generation solution that empowers law enforcement, military, intelligence, personnel to capture critical forensic evidence from Android and iOS mobile devices. With an intuitive touch-screen interface and an integrated battery, Cellebrite UFED Touch is portable, easy to operate, and can be used in the forensic lab and field.

1.1. Overview

Cellebrite UFED Touch enables you to:

» Perform physical, file system, and logical extraction of device data and passwords. Capabilities may vary, based on the Cellebrite UFED Touch product purchased - Cellebrite UFED Touch Logical or Cellebrite UFED Touch Ultimate.

» Extract vital data such as call logs, phonebook entries, text messages (SMS), pictures, videos, audio files, ESN IMEI, ICCID and IMSI information and more, from a wide range of mobile devices.

» Extract data from the widest selection of operating systems, such as Apple iOS, Blackberry, Android, Symbian, Microsoft Mobile, and Palm OS.

» Clone the SIM ID, which allows you to extract phone data while preventing the mobile device from connecting to the network. It can also help if the SIM card is missing.

» Extract the data from a mobile device either by a cable based connection (serial or USB) or a Bluetooth wireless connection. The tips and cable kit consists of four master cables and various tips.

The extracted data can be saved to any standard USB mass storage drive, SD card, or PC, and then generated in the form of clear and concise reports.

Cellebrite's industry expertise provides reliability and ease-of-use, and ensures the broadest support for mobile devices, including updates for newly released models before they are available to the market.

Figure: Cellebrite UFED Touch unit

1.2. Extraction types

Cellebrite UFED Touch includes a range of data extraction types.

> 📄 The available extractions may vary, based on the type of product purchased; the Cellebrite UFED Touch Logical or the Cellebrite UFED Touch Ultimate product.

Table 1-1: Functionalities of the Cellebrite UFED Touch products

Functionality	Cellebrite UFED Touch Logical	Cellebrite UFED Touch Ultimate
Logical Extraction	Yes	Yes
SIM Data Extraction	Yes	Yes
Password Extraction	Yes	Yes
Clone SIM	Yes	Yes
File System Extraction	Not available	Yes
Physical Extraction	Not available	Yes
Capture Images/Screenshots	Optional	Yes
Chat capture	Yes	Yes

The extraction types are:

» **Logical extraction:** Extracts user data from a mobile device (SMS, call logs, pictures, phonebook, videos, audio, certain application data, and more). Quickest extraction method but least amount of data.

» **SIM card extraction:** Extracts data from a SIM or USIM card.

» **File system extraction:** Extracts files embedded in the memory of a mobile device. Retrieve the artifacts within a Logical extraction, in addition to hidden system files, databases and other files which were not visible within a logical extraction.

» **Password extractions:** Unlocks and displays passwords from a source mobile device.

» **Clone SIM:** Copies a SIM ID from one SIM card to another SIM card or to a Cellebrite UFED SIM ID Access Card.

» **Physical extraction:** Extracts a physical bit-for-bit image of the flash memory of a device, including the unallocated space using advanced methods. Unallocated space is the area of the flash memory that is no longer tracked by the file system, which may contain images, videos, files, and more.

» **Capture images and screenshots:** Take pictures or videos of a device using the Cellebrite UFED camera. You can also capture internal screenshots directly from the connected device.

» **Chat capture:** Chat Capture is an automated screen capturing process that allows users to extract and analyze selective chat conversations from third party application data.

1.3. Accessories

The Cellebrite UFED kit includes connection cables and tips. These are used in order to connect mobile devices to Cellebrite UFED.

Figure: Cellebrite UFED Cables and tips

The Cellebrite UFED Ultimate kit contains tips and cables for logical, file system, and physical extractions.

The Cellebrite UFED Logical kit contains tips and cables for Logical Extraction only.

1.3.1. Using cables and tips

The cables and tips include various adapter cables (the number of cables depends on the Cellebrite UFED product and kit purchased). Each cable has a letter and name for example: A Adapter – USB.

Figure: Single cable

For easy recognition, the tips are color coded and numbered; the color represents the vendor.

Figure: Cellebrite UFED tip (example)

Before each extraction, the required cable and tip number and color is specified in the **Source** area of the Select Content Types screen.

1.4. Supported devices

To find out which mobile devices are supported in Cellebrite UFED and which data extraction capabilities are available for every mobile device use one of the following:

1. The Cellebrite UFED <version no> Supported Phone List file is delivered with every Cellebrite UFED software version update. The Microsoft Excel file contains two worksheets:

   The **Cellebrite UFED Logical** sheet lists the mobile devices supported for logical extraction.

   The **Cellebrite UFED Physical** sheet lists the mobile devices supported for physical, file system, and password extractions.

2. **UFED Phone Detective** (devices supported for logical extraction only).
3. Cellebrite UFED Supported Devices document in MyCellebrite.

1.5. Cellebrite YouTube channel

For your convenience, a selection of useful videos demonstrating typical workflows and common procedures are available at youtube.com/cellebriteufed.

2. Orientation to the unit

This section describes the layout and components of the Cellebrite UFED unit.

2.1. Top view

Access the Cellebrite UFED application through the touch screen. Navigate the application using your index finger.

The following components can be found in the top panel:

2.2. Back panel

The back panel of the Cellebrite UFED unit includes multiple ports and a security slot.

The back panel includes the following components:

Mini display port   SD card slot   USB ports   Wireless/Bluetooth switch

Recovery button

Power button   Ethernet port   Power jack   Kensington security slot
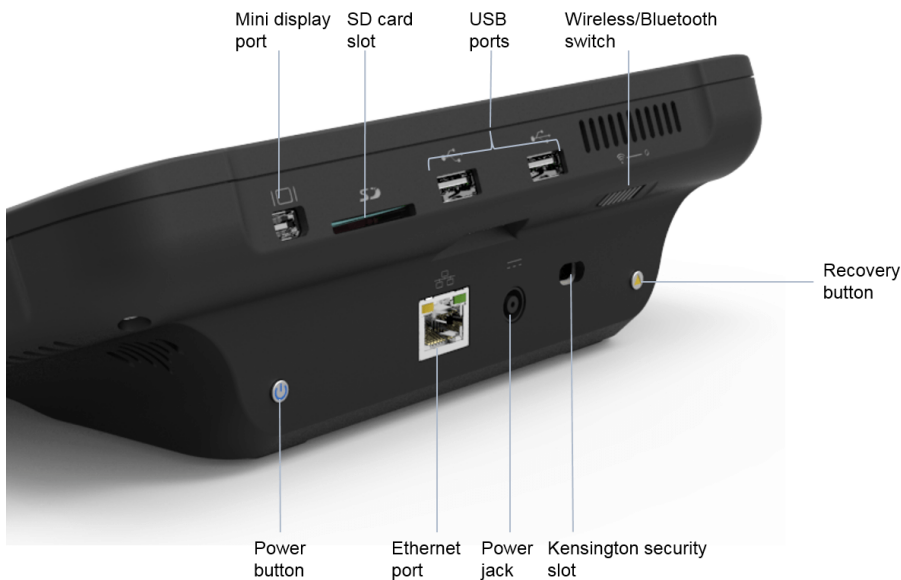
2.2.1. Using the buttons on the unit

2.2.1.1. Power button

Used to turn the system on or off.

To turn system on, the press the Power button.

To shutdown the system, press the Power button until the system starts the shutdown process.

If the system does not respond to the normal shutdown, hold the Power button until the unit turns off.

2.2.1.2. Power button LED

The light is white when the system is on.

There is a blinking orange light while charging.

2.2.1.3. Recovery button

The system supports Recovery mode by means of the Recovery button. In this mode, the system reverts the operating system and all preinstalled software to the factory settings.

To get into recovery mode, do the flowing:

1. The user has to shut down the system.
2. Attach DC power.
3. Press the Recovery button until the button LED starts blinking.
4. Turn on the system within 30 seconds. If 30 seconds timeout reached the system will boot normally.

2.3. Left panel

The left (source) panel of the Cellebrite UFED unit includes the following components:
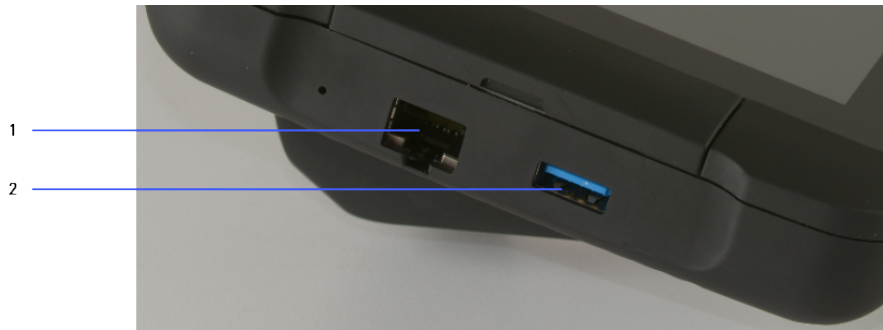
1	Source RJ-45 port
2	Source USB port

2.4. Right panel

The right (target) panel of the Cellebrite UFED unit includes the following components:

1   Target USB port

2.5. Bottom panel

Access to the unit's battery is through the bottom panel.

The bottom panel includes the following component:

2.6. Cellebrite UFED unit case

Protective cases are available for the Cellebrite UFED unit.

2.6.1. Standard case

To insert the Cellebrite UFED unit in the standard protective case:

1. Place the case face up on a flat surface, lift the cover to expose the cavity, and gently insert the Cellebrite UFED unit into the case, as shown.

2. The cover **must** be folded over so that all ports and vents on the back of the Cellebrite UFED unit are fully exposed, as shown.

2.6.2. Ruggedized case

To insert the Cellebrite UFED unit in the ruggedized protective case:

1. Place the case face up on a flat surface.

2. Lift the cover to expose the cavity.

3. Gently insert the Cellebrite UFED unit into the case, as shown.

> 📑 The cover can be unfolded and placed over the Cellebrite UFED unit screen as a visor for outdoor use, as shown.

2.6.3. Replacing the cover

If you need to replace the cover, contact Cellebrite for a replacement.

To replace the cover:

1. Remove the Cellebrite UFED unit.
2. Remove the pins and cover.
3. Insert the tabs into the slots on the back of the cover.
4. Insert the pins into the holes on the edge of each tab, with the pin head up.
5. Press the pins into the hole under the slots - view the case from the inside and apply pressure to the pins until secure.

3. Getting started

This section includes the following:

3.1. Turning the unit on or off

The power button for the Cellebrite UFED unit is located at the back of the unit.

Figure: Cellebrite UFED right panel – Power button

To turn the Cellebrite UFED unit on:

» Push the power button located at the back of the unit.

The unit lights up and the startup sequence begins.

During the startup sequence:

» The operating system (Microsoft Windows) starts automatically.
» The Cellebrite UFED application starts automatically.

To log off, restart or shut down the Cellebrite UFED:

» Tap **Settings** > **Shut down Options** (tab) and then tap **Log off**, **Restart** or **Shut down**.
» To perform an immediate shut down, push the power button and hold it until the device powers down.

3.2. Starting the application manually

When you turn on the Cellebrite UFED unit, the Cellebrite UFED application is launched automatically. If the application does not launch automatically or if you had to previously quit, use one of the following to launch the application:

» Tap the **Cellebrite UFED application** shortcut located in the shortcuts panel at the right of the screen.

» Double-tap the **Cellebrite UFED** icon located on the desktop.

3.3. Home screen

The home screen groups the extraction data into distinct areas: Mobile device, SIM card and USB device or Memory card. In addition, users can directly operate the camera for immediate image capturing or access the device tools. All extraction functionality is driven by **automatic** identification of the device, by **searching** for the device or by **manually** selecting the vendor and model. Cellebrite UFED determines what functions are available for the specific device and displays the relevant functions.
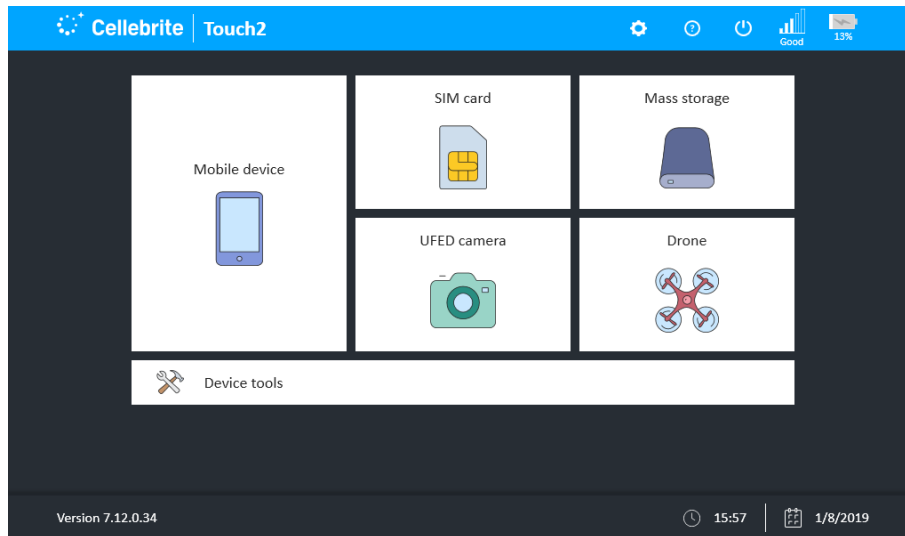
3.4. Autodetecting a device

To use Autodetect to locate the mobile device:

1. Connect the mobile device to the Cellebrite UFED unit.
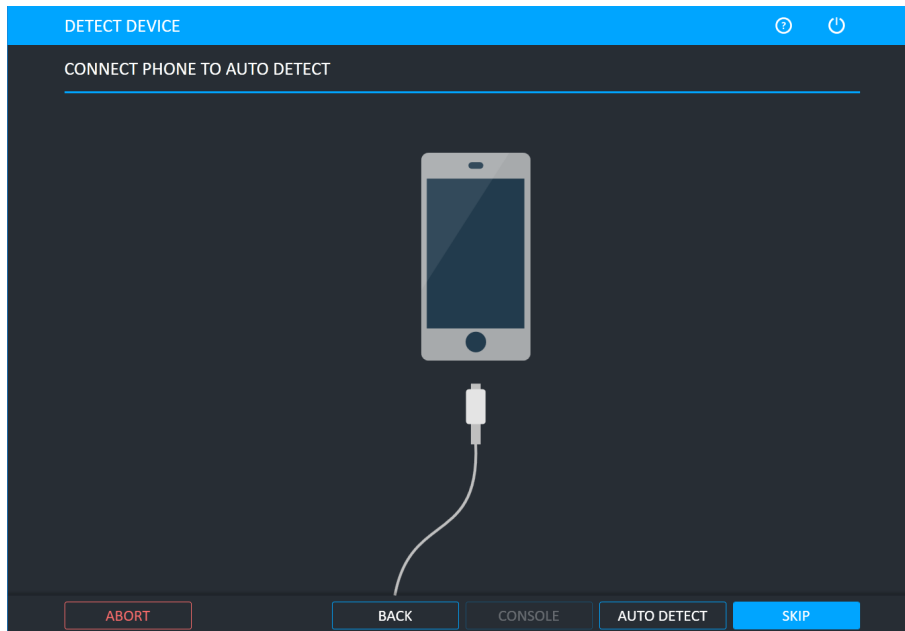
2. Tap the device.

3. In the event that the device has not been connected, a red Source arrow (◀) flashes on the left side of the screen.

   If the connected device is recognized by the system the following window appears.
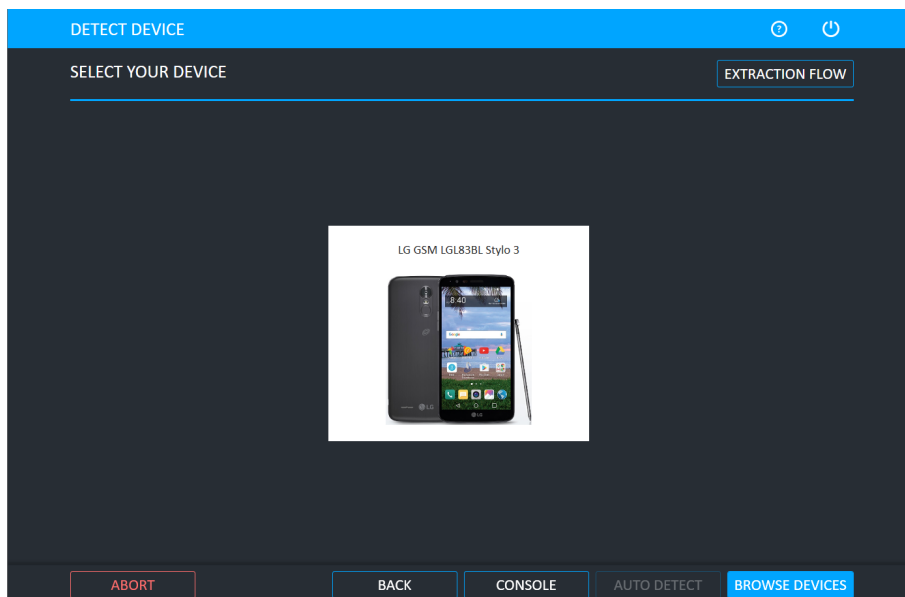
If multiple matches are found, the following window appears.
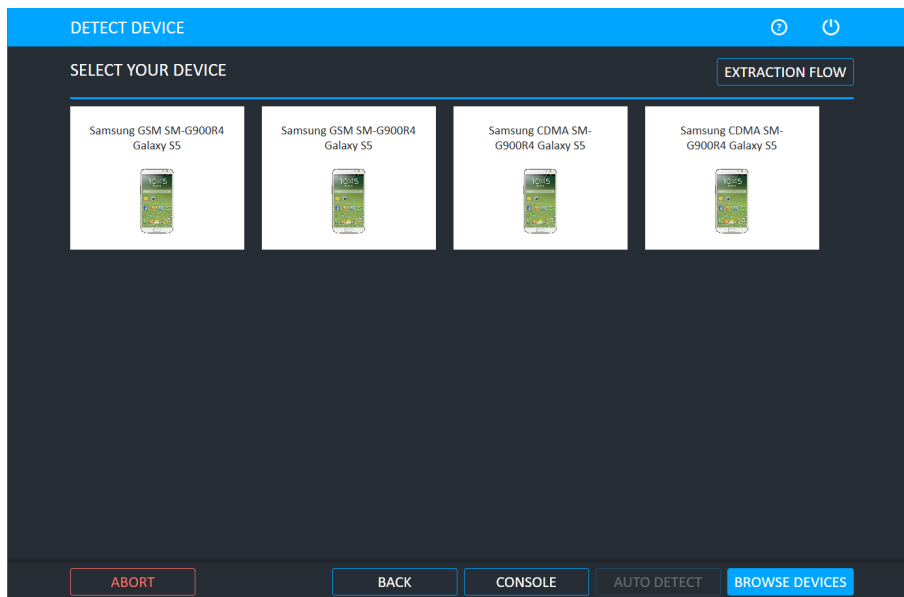
4. Select the relevant device.

5. Alternatively, tap **Browse Devices** to manually search for the device.

> Click the **Console** button to access device information using the Android Debug Console. For more information, refer to the *Performing extractions* manual.

6. If the connected device cannot be recognized by the system, a message prompts you to try the following steps or tap Find device manually.
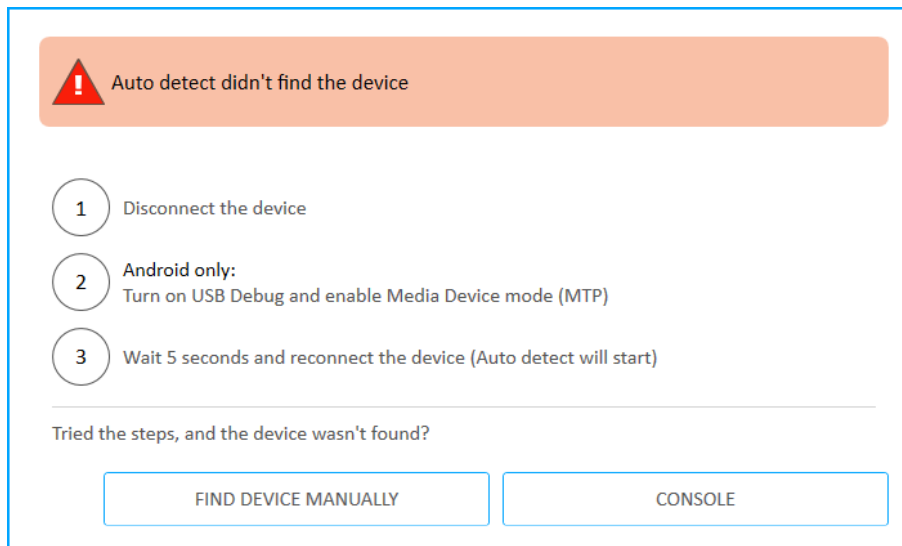
7. If the device still cannot be found, tap **Browse Devices** or **Console**.

3.5. Searching for a device

To search for the mobile device:

1. Narrow the list by vendor, recently used, etc. or begin typing in the search box in the top bar to search for a device or model. As you type, the list of devices is reduced to match your search criteria.
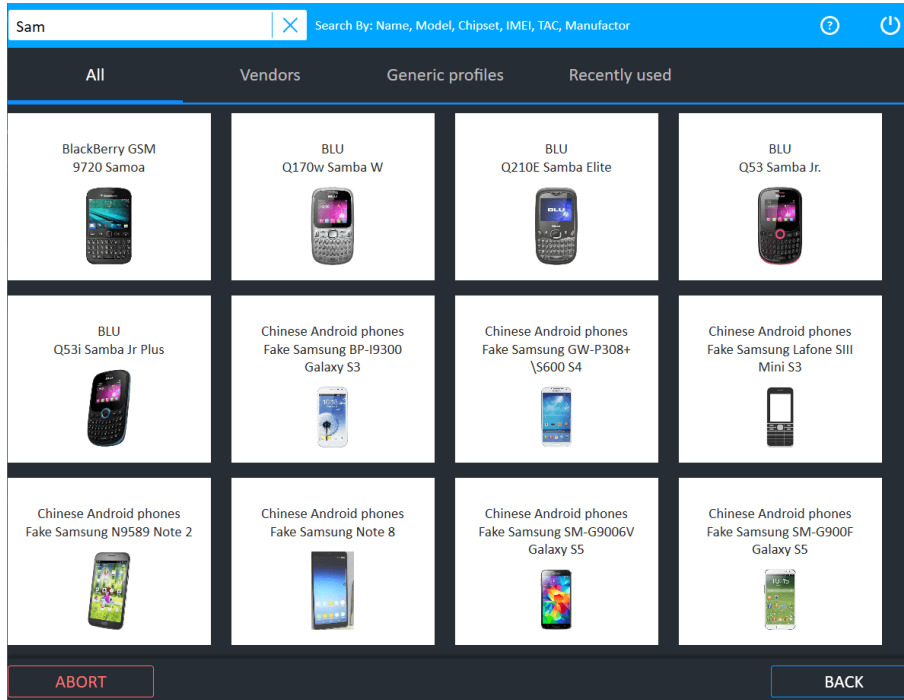
> 📄 You can also search for a device by its IMEI value, which is used to uniquely identify devices. The IMEI value is usually found printed inside the battery compartment of the device, or dial *#06# from the phone keypad. Enter the value in the search box, using a minimum of four digits up to the full number. If the IMEI value is recognized, matching devices will be displayed.

2. Select the device model type from the list.

Having selected the **device**, Cellebrite UFED will determine what extraction functions are available for this combination and present those functions as follows:
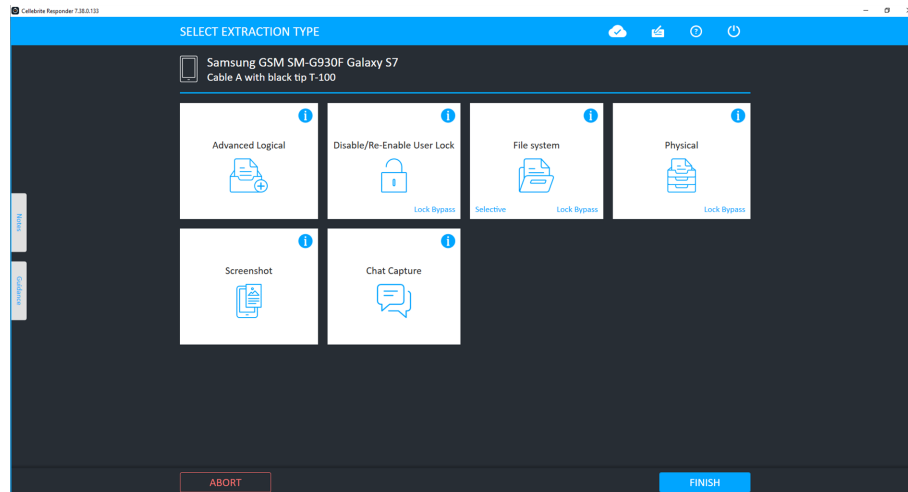
> Lock Bypass is displayed for both physical and file system extraction methods that can bypass the user lock of the device.

3.5.1. TAC search

If you cannot find the Android device which you are looking for after performing a TAC number search, a window will appear. This window appears if Cellebrite UFED does not support the device directly, but there are applicable generic options available for the device.

To retrieve device information and view generic extraction options:

1. Enter the complete 8-digit TAC number. The following window appears.

The window includes the vendor, operating system and device name.

2. Tap **See recommended extractions**. A window appears with the generic extraction options for the device. An example appears next.

Smart Phones/PDAs MS Windows Mobile 6.x
using Cable A with black tip T-80 or T-100

Logical	Physical	Camera

ABORT   BACK
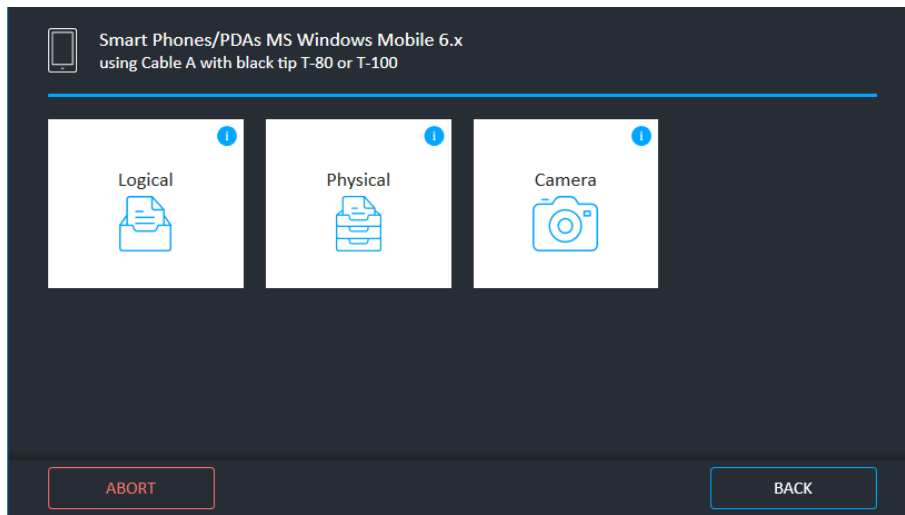
If you enter a partial TAC number (with less than 8-digits) or the device is not supported by Cellebrite UFED then the following window appears.

3568588   X   Search By: Name, Model, Chipset, IMEI, TAC, Manufactor

All   Vendors   Generic profiles   Recently used

It appears that this device is not supported by UFED. Enter the complete 8-digit TAC to retrieve device information and extraction recommendations.

ABORT   BACK
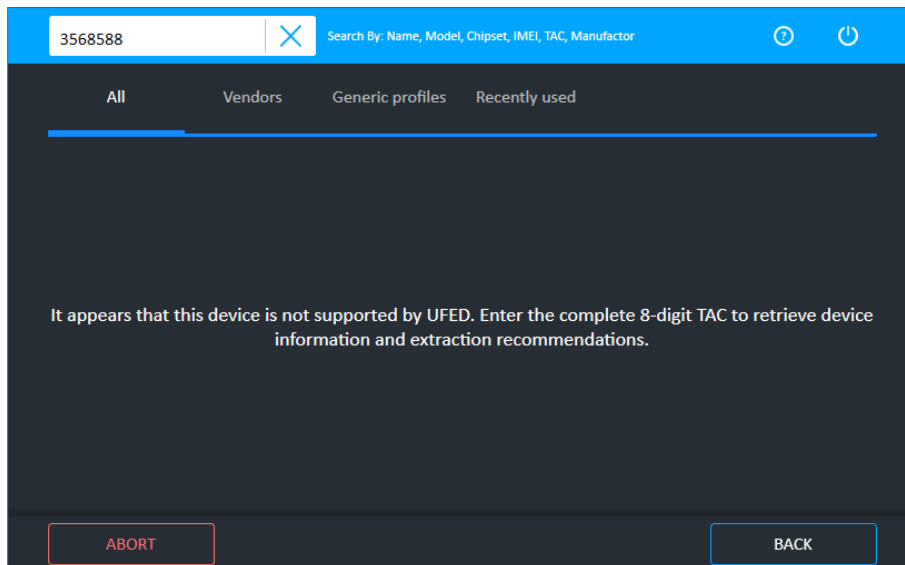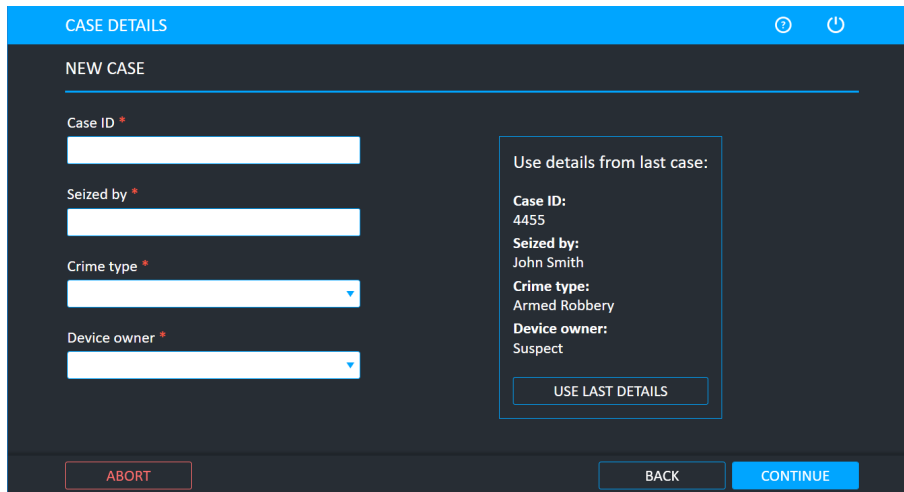
3.6. Case details

The Case details feature enables you to enter case details when performing an extraction or using the Cellebrite UFED camera. This feature is not enabled by default.

To enable the case details feature:

» Select **Include Case details screen** under **Settings** > **General**. For more information, see General settings (on page 54).

To specify the case details:

1. On the Home screen, select an extraction type or Cellebrite UFED camera. The following window appears.

2. Use the current case information, or enter and select the case information and then tap **Continue**.

> 📄 The Crime Types list can be changed via the Cellebrite UFED Permission Manager (Using the Cellebrite UFED Permission Manager (on page 90)) or Cellebrite Commander (refer to the Cellebrite Commander manual).

3.7. User predefined filter

The User predefined filter provides the ability to extract and view only a portion of the device content, based on time range or specific subject information (person, email, phone). This can be useful when:

» The agency has a warrant to extract data from a specific time window, and is not allowed to view additional data that is not covered by the warrant.

» The user wishes to save time and get to the relevant data ASAP.

The most time consuming phase during a device extraction is transferring the data from the mobile device to the extraction tool. Timeframe filtering is performed on the device (when technically supported), and can reduce the extraction time. Another advantage is the reduced amount of data that the agent needs to browse through in order to find the evidence.

To enable the User predefined filter:

» Select **Allow user predefined filter** under **Settings** > **General**. For more information, see General settings (on page 54).

To specify the timeframe and parties for the extraction:

1. Identify the device and select an extraction type. The following window appears.
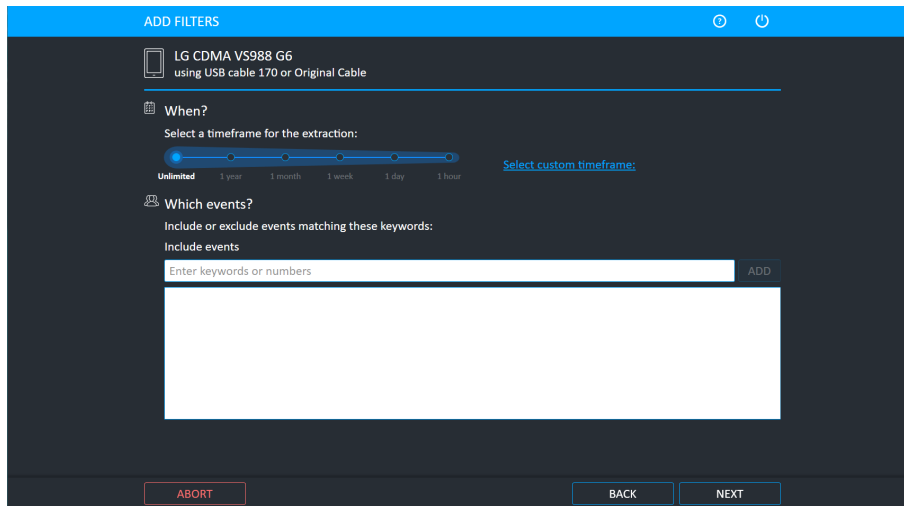
> 📑 The extraction is based on the Cellebrite UFED unit's date and time. When selecting a time frame you should also consider the device's time zone.

> 📑 The timeframe option is not applicable to file system extractions.

2. Select the required time frame. The less time selected, the quicker the extraction.
3. Enter keywords or numbers that you would like to include.

> 📄 Selective extraction by party: Similar to the time frame, the ability to extract and review only data relevant to a specific party (number or device).

> 📄 Partial numbers will be matched by the application, and names are matched irrespective to the capitalization.

4. Tap **Next**.

3.8. Manual selection

To manually select the vendor and model:

1. Tap **Mobile device** and then tap **Skip**.

   You can then select **All**, **Vendor**, **Generic profiles**, or **Recently used**. As displayed next, the Vendor screen enables you to select the device vendor.
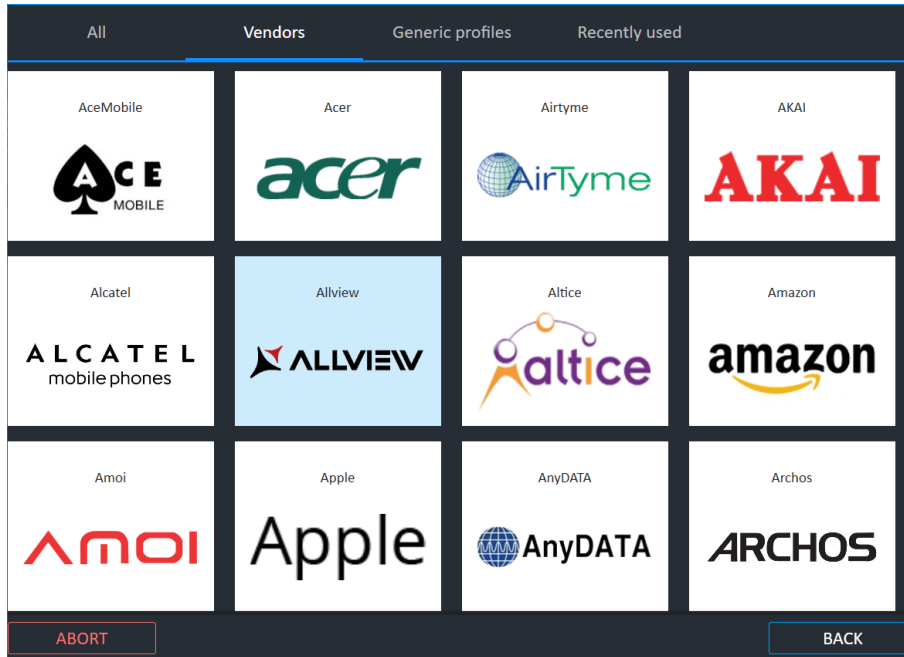
2. After choosing the Vendor, the application presents the Select Model screen where the specific model of the device is chosen:
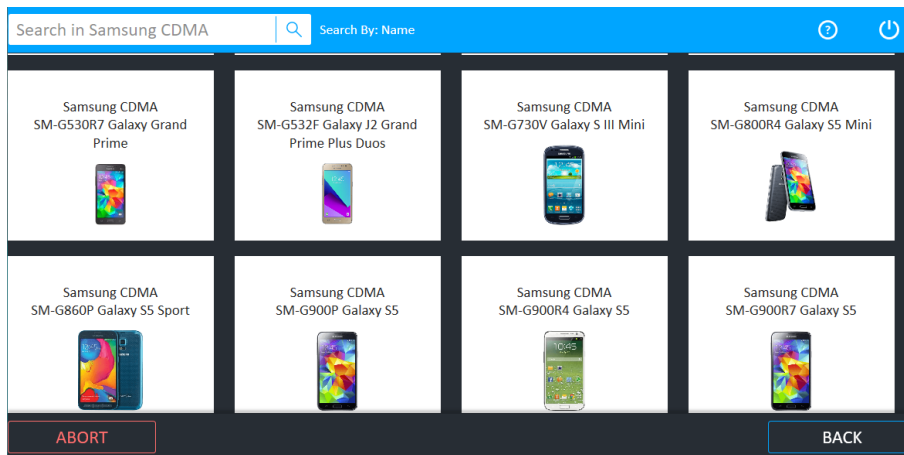
   Having chosen the **Vendor** and the **Model**, Cellebrite UFED will determine what extraction functions are available for this combination and present those functions.

3.9. Application taskbar

The application taskbar is located at the top of the screen.

Application taskbar icons and descriptions

Icon	Description
	Wireless network connection (= Disconnected, = Connected).
	Display the Settings screen from where the device settings can be defined.
	Exit, lock or log off.
	Display the online Help.
	Battery indicator.

3.10. Virtual keyboard

The virtual keyboard allows you to type text whenever needed.
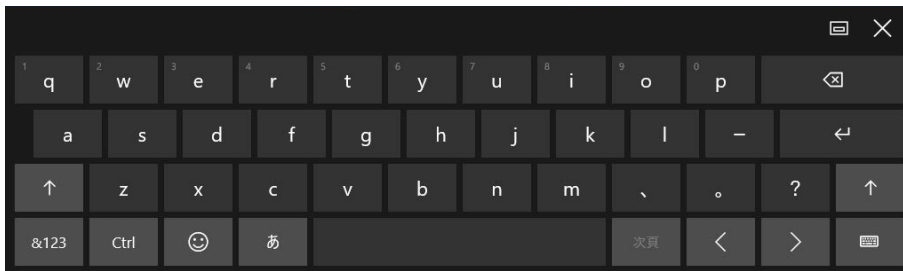
Figure: Virtual keyboard

» To show the virtual keyboard, double-tap any text box requiring input.
» To close the virtual keyboard, tap the X icon in the top right corner of keyboard panel.

Table: Virtual keyboard icons and descriptions

Icon	Key Function
&123	Switch to numbers and symbols mode
↵	Create a new line
⌫	Delete the last character
↑	Activate CAPS LOCK

> Any external USB keyboard can be connected to a USB port in the back panel, or a Bluetooth keyboard paired with the Bluetooth interface of the device.

3.11. Waking up from sleep mode

The Cellebrite UFED unit enters sleep mode after being idle for 20 minutes in order to reduce power consumption.

To wake the unit up:

» Tap the touch screen.

3.12. Charging the battery

To charge the Cellebrite UFED battery, connect the supplied power adapter to the power supply jack at the back of the device.

3.13. Enabling wireless and Bluetooth communication

The Cellebrite UFED unit is equipped with integrated wireless and Bluetooth communication interfaces, configurable in the operating system Device Manager list, and can be used to connect Cellebrite UFED to standard WLAN networks and Bluetooth-enabled devices using the standard WLAN and Bluetooth features of the operating system.

> For information regarding the use of Wi-Fi/Wireless Networks and the operating system's wireless features, contact your IT manager or system administrator.

When using the wireless interfaces when the device is in battery operation mode increases battery power consumption, resulting in a shorter operation time. When the wireless interfaces are disabled, the WLAN and Bluetooth interfaces are turned off and cannot be turned on or used by the operating system, thus saving battery power.

To enable or disable the wireless interfaces:

» Turn the Wireless/Bluetooth switch, located in the back panel of the Cellebrite UFED unit, to **ON** or **OFF**.

4. Activating the license

If your Cellebrite UFED unit is not already activated, you need to activate the license.

To activate the license:

1. Power on the Cellebrite UFED unit.
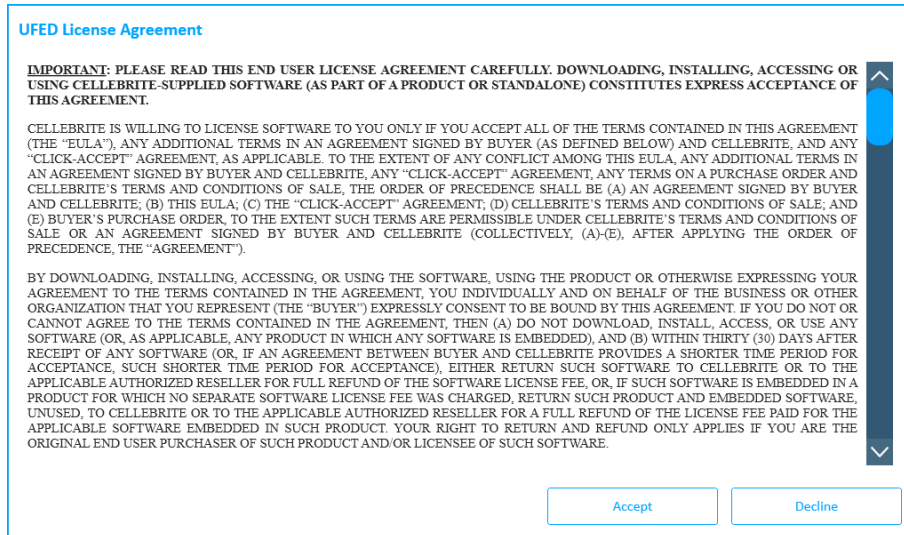
2. Tap **Approve**. The following window appears.
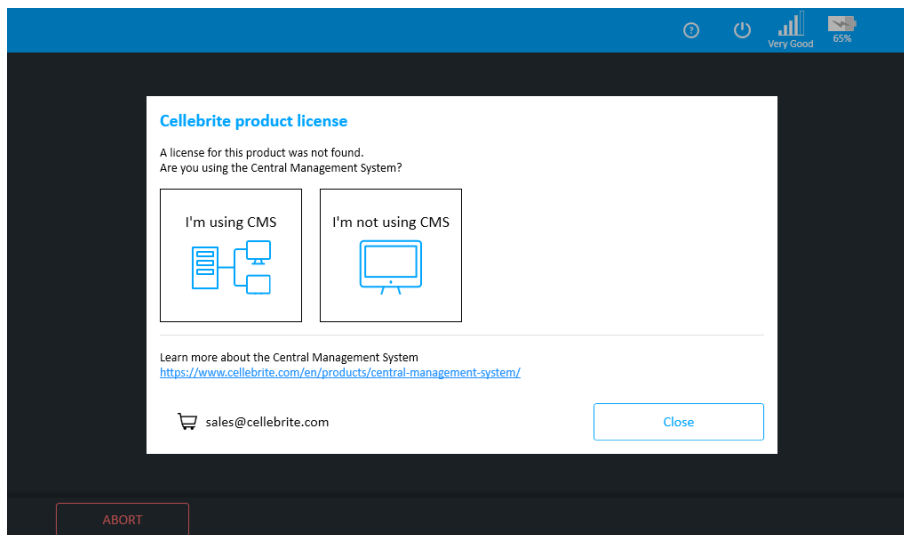
If you are using Cellebrite Commander:

1. Click **I'm using Cellebrite Commander**. The following window appears.

Cellebrite product license
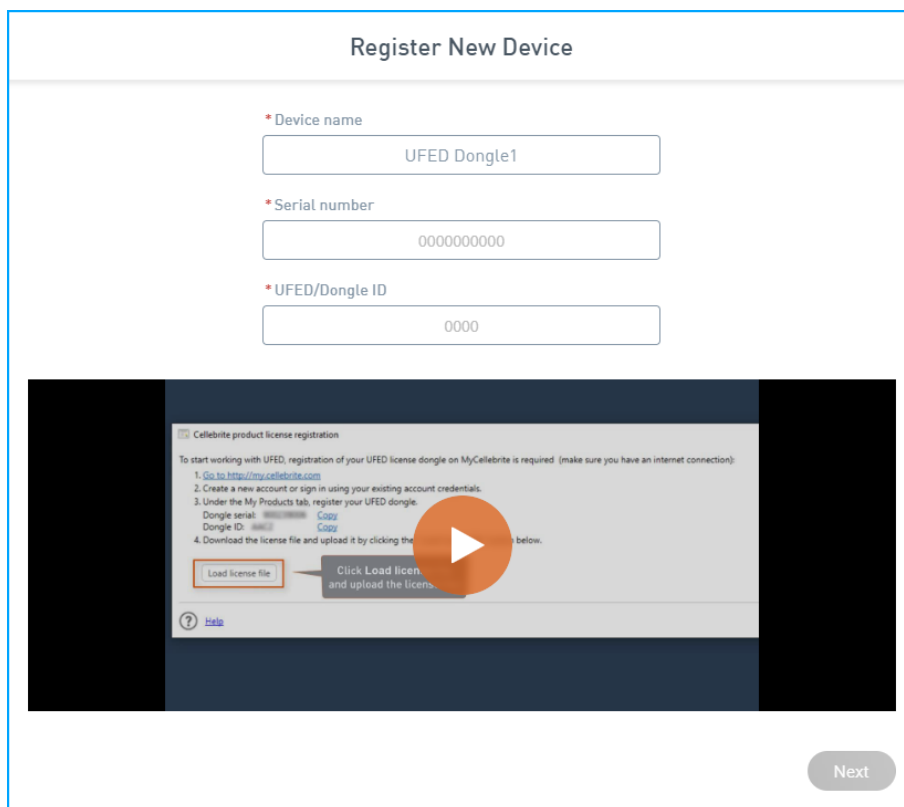
Connect to your Centralized Management System (CMS) server

CMS Server:

http:/ubuntu.local   Validate

If you have a license dongle, connect it before validating

Status:
Connection not initiated

⑦ Help   🛒 Sales   Back   Close

2. Enter the Cellebrite Commander Server information. For more information on entering the information in this window, see Connect a Cellebrite UFED device to Cellebrite Commander (on page 70).

3. Click **Validate**.

If you are not using Cellebrite Commander:

1. Click **I'm not using Cellebrite Commander**. The following window appears.

2. On a PC, go to community.cellebrite.com and log in with your credentials (or create an account).
3. Go **to Products & Licenses** > **Register Device** and enter a name for the device, the serial and UFED ID as displayed in the Cellebrite product license window.
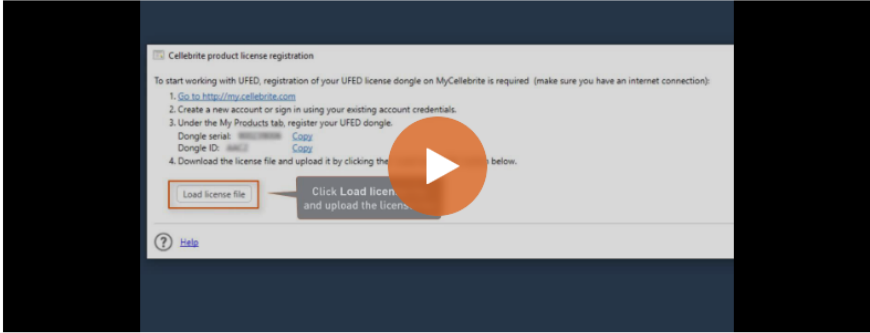
4. Click **Next**. The following window appears.
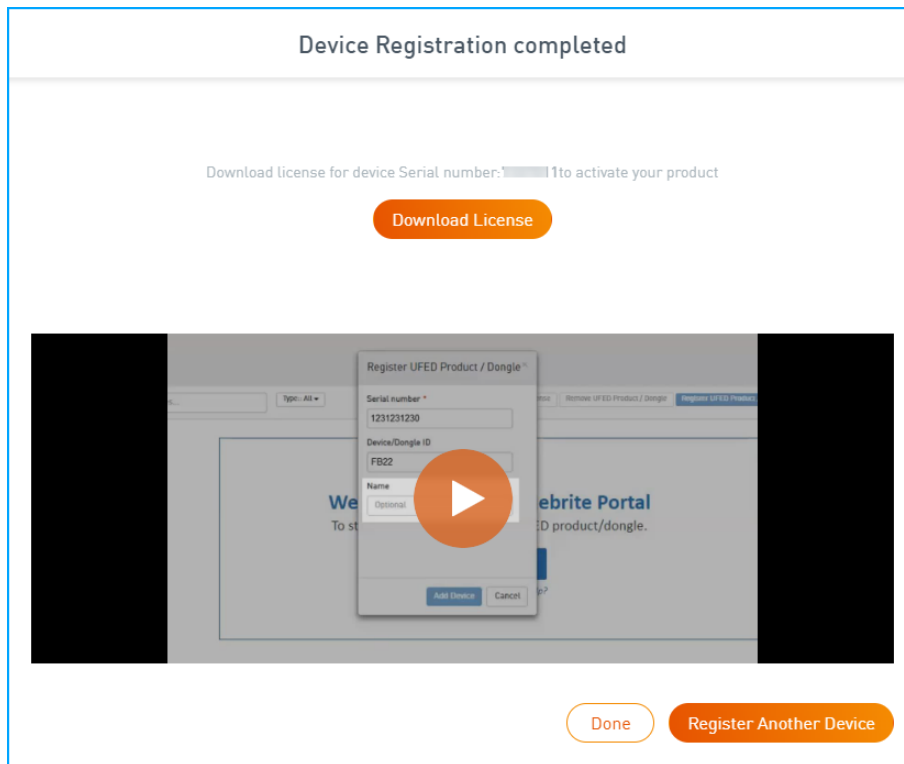
5. Click **Download license** from the Device Registration Completed window to download the license key.
6. Copy the license key to the root directory of a USB flash drive.
7. Insert the USB drive into a USB port at the back of the unit.
8. In the Cellebrite product license window, tap **Load from USB** and upload the license key.

   Congratulations, your Cellebrite UFED unit is now ready!

5. Extracting data to PC

> Extraction to a PC with Windows Vista Operating System is not supported.

1. Do one of the following:
   - » Connect the Cellebrite UFED unit to your PC using a USB to mini-USB cable, utilizing the port marked "PC" located at the back of your Cellebrite UFED unit. Your PC may prompt you to install drivers.
   - » Connect your Cellebrite UFED unit to your PC using the UFED to PC cable (USB3 Host-to-Host cable) provided in the Cellebrite UFED Standard and ruggedized kits. Your PC may prompt you to install drivers.

Figure: USB3 Host-to-Host cable

2. Connect the source device, using the appropriate cable, to the Target USB port of the Cellebrite UFED unit.
3. On the Cellebrite UFED unit, select Extract from Mobile device and identify the device, then select the extraction type.
4. On the PC, click **Start** > **Physical Analyzer** to open the Physical Analyzer.

   The **Physical Analyzer** application starts.

5. Click the **Read Data from UFED** icon in the application toolbar.

The **UFED Downloader** window appears.
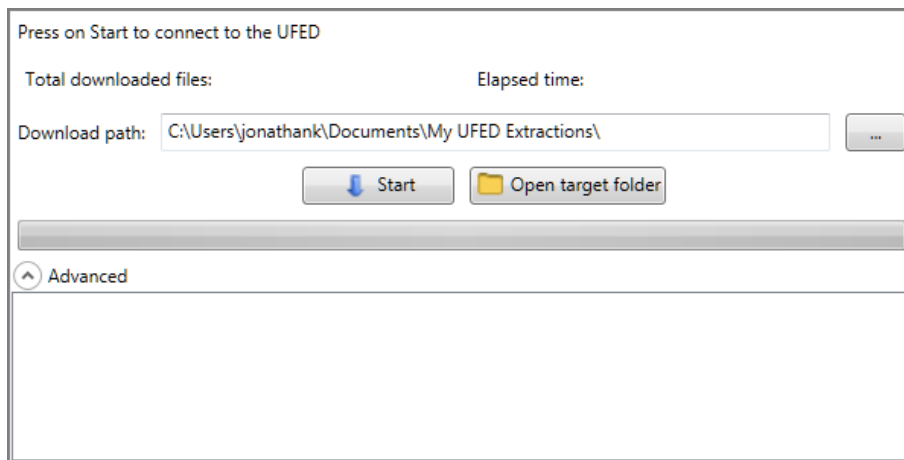
6. In the **Download path** area, click [...] and browse to the desired location for the extraction.

   Tip: Click **Open Target Folder** to display the content of the selected target folder.

7. On the Cellebrite UFED unit, in the Select Extract Location screen, select **PC**.

8. Follow the prompts in the Cellebrite UFED unit until prompted to start the download procedure.

9. On the PC, in Physical Analyzer, click **Start** in the Cellebrite UFED Downloader window.

The data transfer from the device to the PC starts.

Press on Start to connect to the UFED

Total downloaded files: 8   Elapsed time: 00:02:59

Download path: C:\Users\jonathank\Documents\My UFED Extractions\   ...

                ✕ Stop   📁 Open target folder

⌃ Advanced

ⓘ   Downloading file: Dump/system/fonts/DroidIndia.ttf Size: 1098064 bytes

ⓘ   Current file, Downloaded 1098064 bytes (100%)

ⓘ   Downloading file: Dump/system/fonts/DroidSansArabic.ttf Size: 35880 bytes

ⓘ   Current file, Downloaded 35880 bytes (100%)

ⓘ   Downloading file: Dump/system/fonts/DroidSansMono.ttf Size: 119380 bytes

ⓘ   Current file, Downloaded 119380 bytes (100%)

During the extraction process, the Extraction in Progress screen appears on the Cellebrite UFED unit.

On the Cellebrite UFED unit, you are prompted to select the types of multimedia to include in the extraction:

10. Make sure that the media types that you want to include in the extraction are marked with ✓. To cancel the extraction of a particular multimedia type, click ✓ on the multimedia name.

11. Click OK.

The extraction process continues. When complete, the Extraction summary screen appears on the Cellebrite UFED unit.

On the PC in Physical Analyzer, the message appears requesting if you would like to open the extraction:

12. Click **Yes**.

The extraction opens in Physical Analyzer and the Extraction Summary screen is displayed.
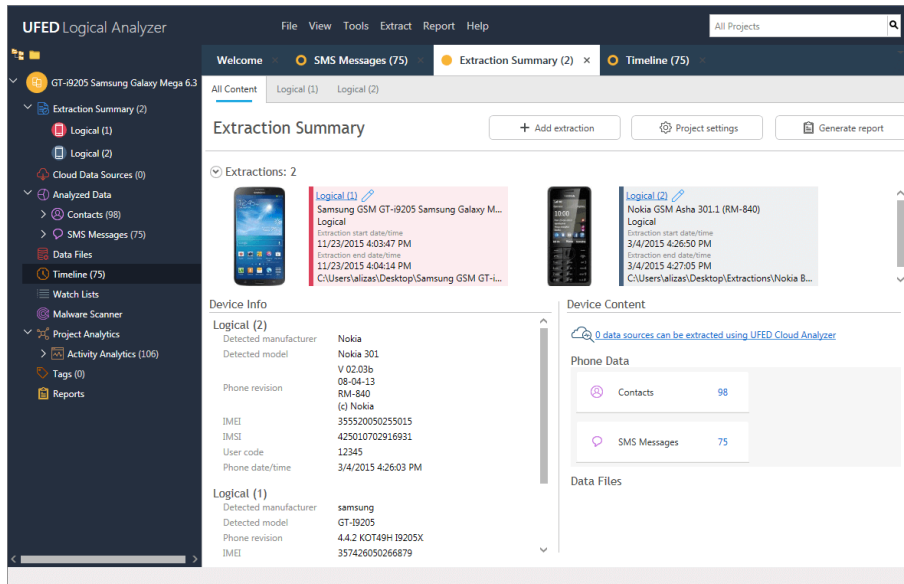
6. Advanced logical Android extraction

The following procedure explains the Advanced logical extraction process for an example device. The procedure may vary depending on the selected device. This section shows only one of the many extraction types that can be performed.

To perform a logical extraction from a mobile device:

1. Tap **Mobile device** and identify the device, then tap **Logical Extraction**.

> 📄 For information on using optional timeframe and party filters, refer to the *Overview Guide*.

The Select Extraction Location window appears.
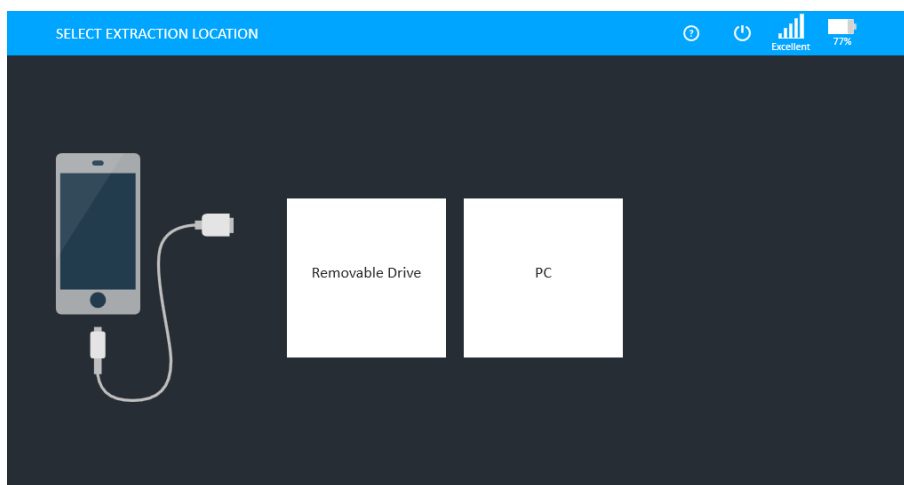
2. Select the desired target location as follows:

   » Select **Removable Drive** to extract the device data to a USB Flash drive connected to the Cellebrite UFED TARGET USB port (on the right panel) or SD card inserted to the SD card reader (on the back panel).

   » Select PC to extract the information directly to the PC. The Physical Analyzer Application must be installed on the PC before the PC option can be selected. See Extracting data to PC (on page 42).

   The Waiting for Device window appears.
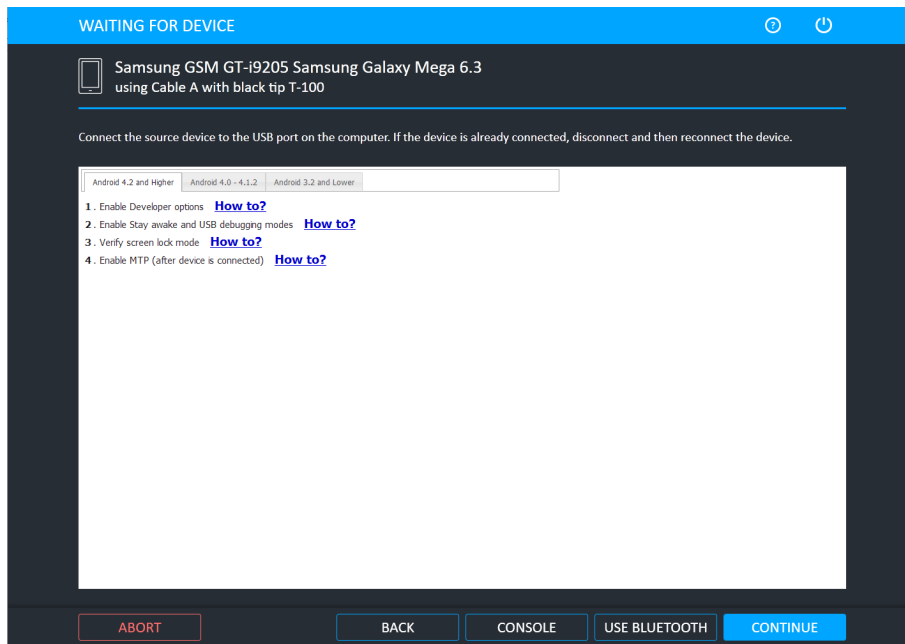
3. Select the correct cable and tip for the mobile device, and change the device settings according to the instructions.

4. Connect the source device to the USB port on the unit. If the device is already connected, disconnect and then reconnect the device.

5. Tap **Continue**. The following window appears if the Enable device preview info screen option is enabled under General settings.
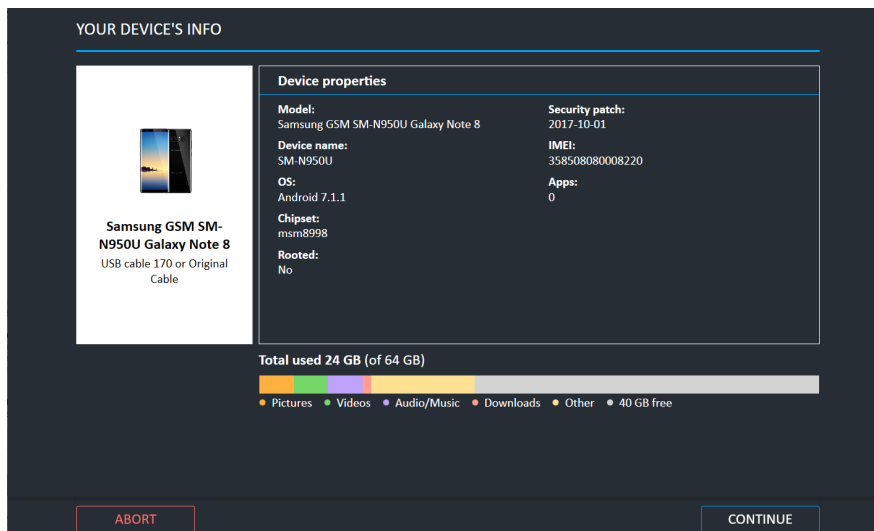
This window provides information on the device data before performing an Android extraction. It includes device properties such as model, device name, OS, chipset, whether the device is rooted, date security patch installed, IMEA, the number of installed apps, and insights from installed apps.

Insights from installed apps allows the user to get a peek into the types of apps installed on the device before the extraction. This areas displays app categories and the number of apps in each. Click [View all] to view all app insights by category.

To update the app categorization database, see
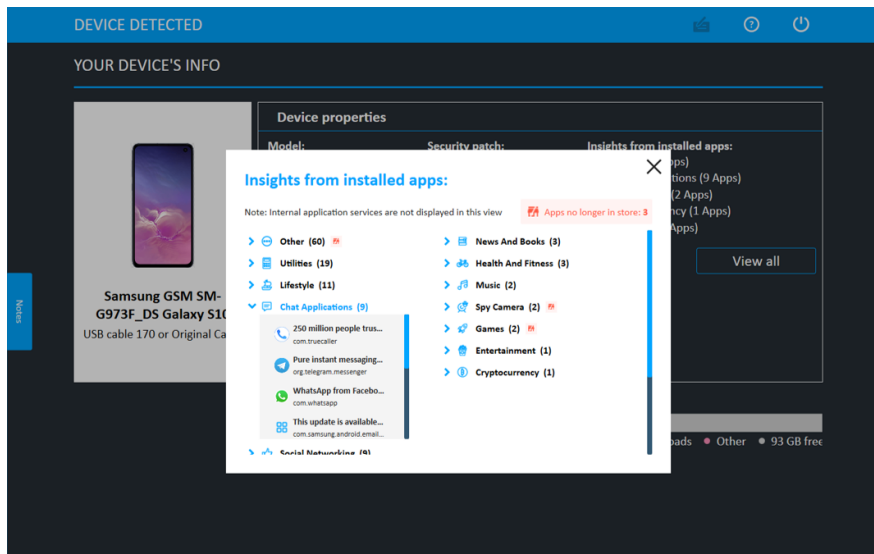
On many devices, but not all it also includes information on storage volume, data types, volume of storage per data type, and free data.

6. Tap **Continue**. The following window appears.
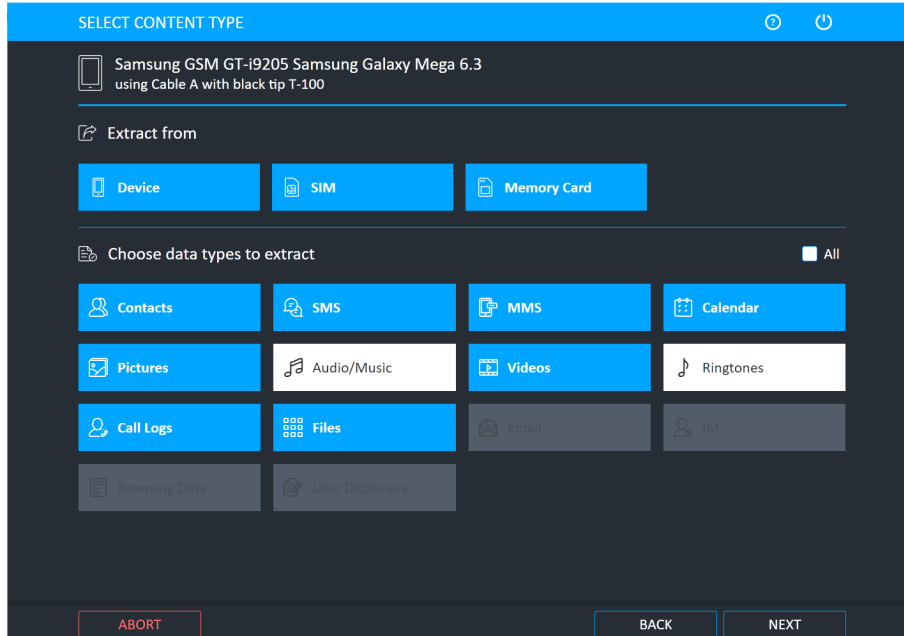
> 📄 Click the **Console** button to access device information using the Android Debug Console. For more information, see AndroidDebugConsole.htm.

7. Data can be extracted from the Device, SIM and Memory Card of the device. Select from which memory you want to extract, select the data types required and then tap **Next**.

8. Different data types can be extracted. Select which data types you want to extract. In the example above, music and ringtones are excluded and will not be extracted.

> 📄 When Files is selected, Cellebrite UFED performs ADB backup to enable user data to be extracted. If you are performing an iOS extraction, Cellebrite UFED performs an iTunes backup.

9. Tap **Next**. The following window appears.

Extract Contacts

Select the accounts for extracting contacts:	Contacts	Estimated time
✓ **PHONE** contacts	104	00:00:18
✓ **GMAIL** kat.cheme1610@gmail.com	1	00:00:01
✓ **FACEBOOK** messenger	1	00:00:01

Continue

10. Select the required contacts to extract and tap **Continue**. The extraction process starts.
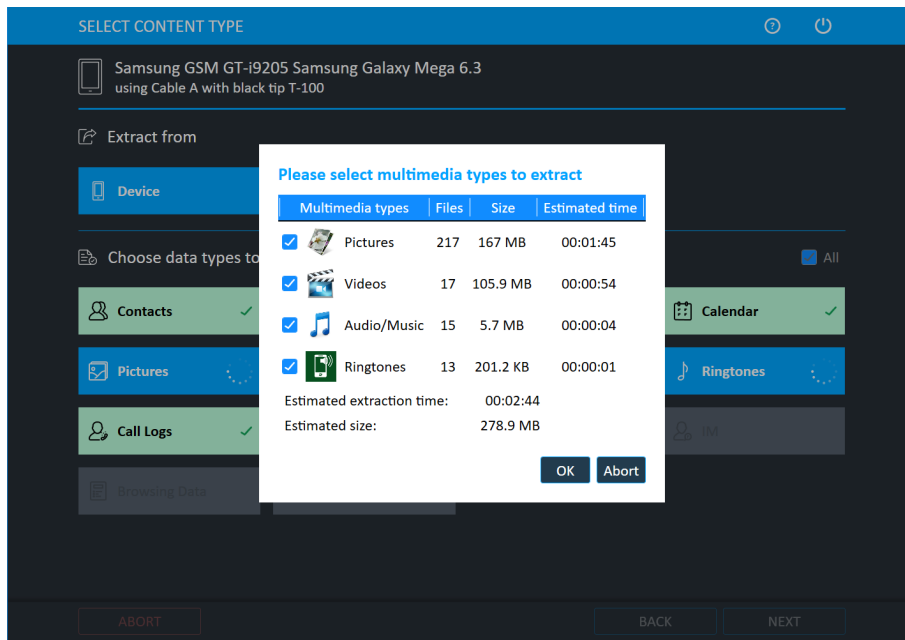
11. Tap **OK.** The following window appears.
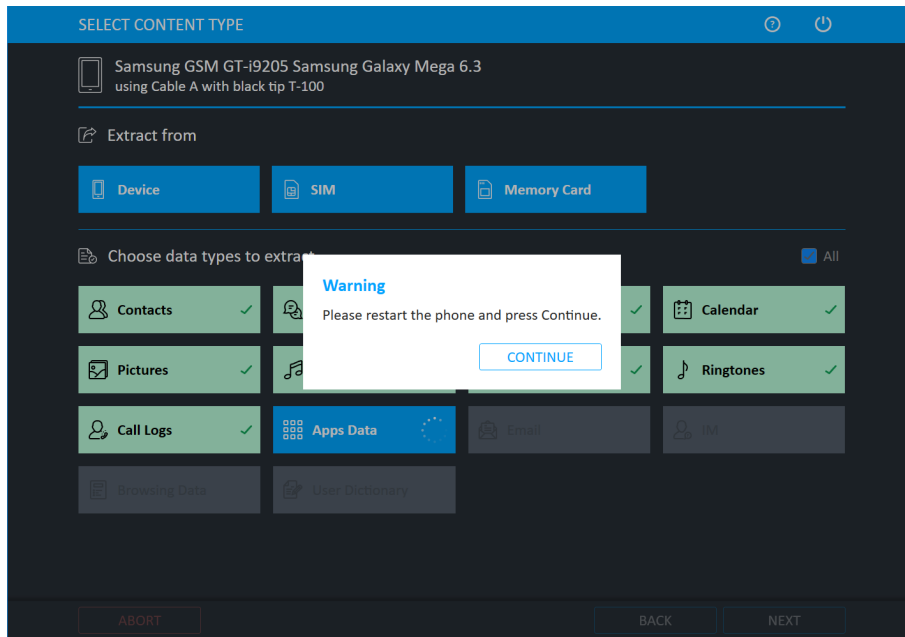
12. If required, restart the device then tap **Continue**. When the extraction is complete and if required, the Source Instructions window appears (this depends on the device model). The following window appears.
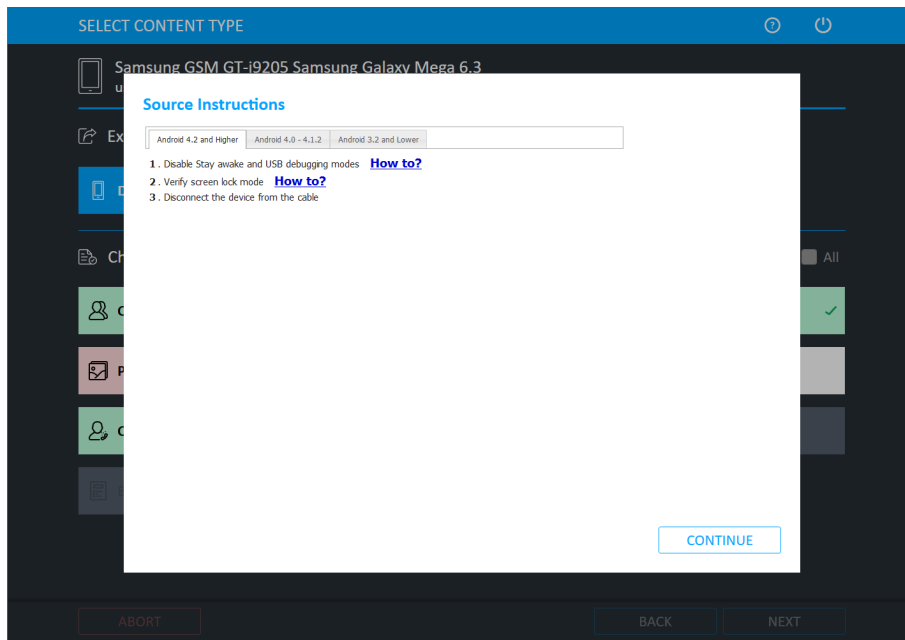
13. Follow the instructions to return the mobile device settings to the correct settings, and then tap **Continue**. The following window appears.
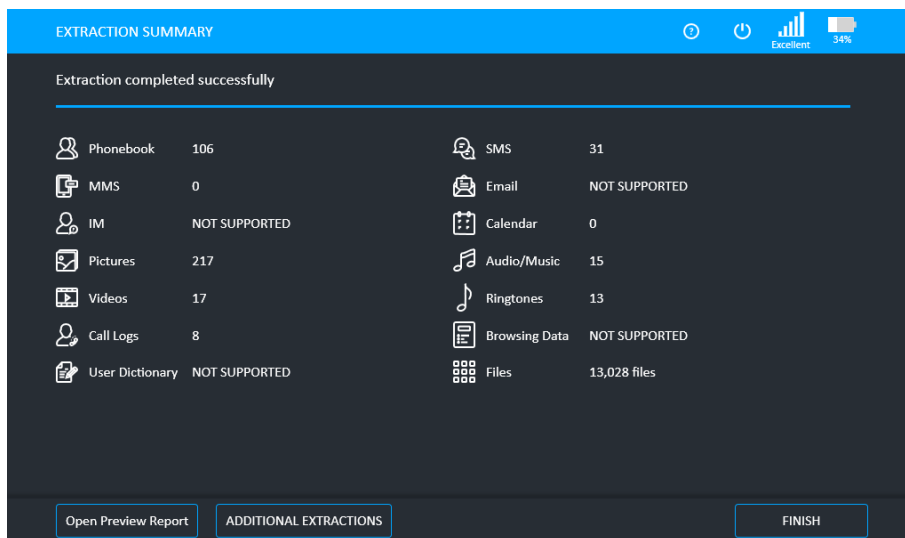
14. Tap **Open Preview Report** to view an HTML preview report that includes information about the device and the extraction, tap **Additional Extractions** to add additional extraction types for the same device or tap **Finish** to end the process and return to the Home screen.

An example of a preview report is shown next.

Phone Examination Preview Report Properties

Selected Manufacturer:	Samsung GSM
Selected Model:	GT-i9205 Samsung Galaxy Mega 6.3
Detected Manufacturer:	samsung
Detected Model:	GT-I9205
Revision:	4.4.2 KOT49H I9205XXUDOA1
IMEI:	357426050266879
Extraction start date/time:	15/02/2017 11:58:56
Extraction end date/time:	15/02/2017 12:14:59
Phone Date/Time:	15/02/2017 11:59:21 (GMT+2)
Connection Type:	USB Cable
UFED Version:	Product Version: 6.1.0.13 , Internal Build: 4.5.2.13 UFED
UFED S/N:	56OAKCLQPHAIYYOKSFCNC

Note: This device is using client in order to communicate with UFED

For complete analysis and advanced reporting, open in UFED Physical/Logical Analyzer.

•**Generic Extraction Notes:**
+ZZ – Extracted phone time stamp time zone is expressed in quarters of an hour
Last IMEI digit might be incorrect. Please check manually on the device.

6.1. The extracted data folder

At the end of the data extraction process, the extracted data is saved in the location you selected.

> The extracted data folder is named "UFED" with the selected device name, the IMEI/MEID info. and the extraction date. For example, "UFED Samsung GSM GT-i9205 Samsung Galaxy Mega 6.3 2014_11_10 (0001)"

The extracted data folder contains:

» Multimedia files folders named Audio, Images, Ringtones, and Video folders, containing each of the respective type of media files.
» Phone extraction report files in HTML and XML formats. (One HTML report per content type)
» Cellebrite UFED Manager files of the extracted calls log (*.clog), phonebook (*.pbb), SMS messages (*.sms), and calendar (*.cal) Email(*.Email), MMS(*.MMS) and IM(*.IM) data.
» UFD file.

> UFED Manager files are generated only for data types that contain items.

The XML file can be viewed by both Logical Analyzer and Physical Analyzer.

7. Settings

The settings screen provides access to a set of functional and behavioral setup options used to control the functionality and usability of Cellebrite UFED.

To access the settings screen, tap the menu icon in the application taskbar and select Settings..

The settings are grouped in the settings screen in the following tabs:

- General settings (on the next page)
- Report settings (on page 61)
- System settings (on page 65)
- License settings (on page 67)
- Version details (on page 70)
- Activity Log (on page 79)
- Users permissions (on page 81)
- Network (on page 95)

The settings screen opens on the **General** tab.

> When using the Cellebrite Commander, some or all of these settings may be managed by Cellebrite Commander.

> Changes that are made to the settings via Cellebrite Commander or manually by a user, will affect all users on the same machine.

7.1. General settings

The settings screen opens on the **General** tab.
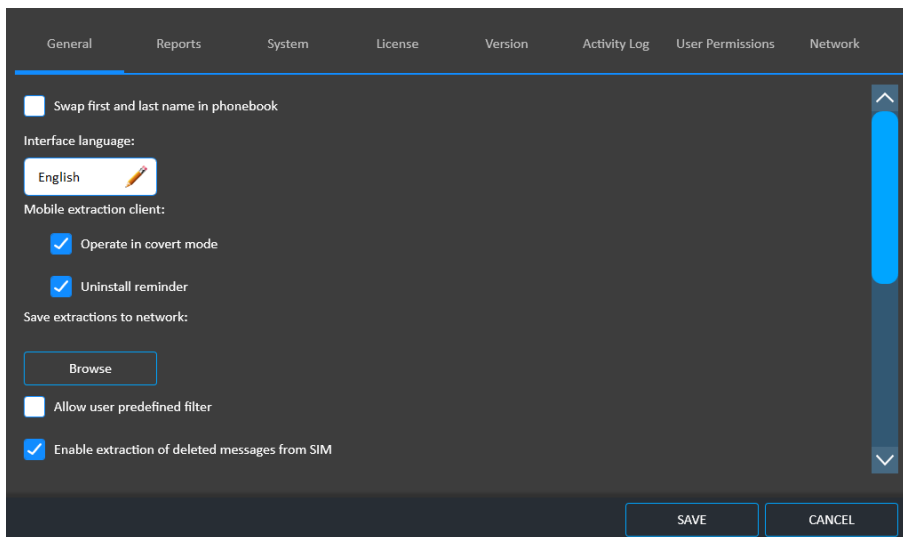
The **General** tab provides access to the following functions and settings:

Setting	Description	Default
Swap first and last name in phonebook	Swaps the first and last name in phone book entries.	Selected
Interface language	Changes the interface language. For more information, see Changing the application interface language (on page 58)	English
Operate in covert mode	Renames the application client name from "Cellebrite.sis/exe" to "AAA.sis/exe".	Selected
Uninstall reminder	When enabled, the Cellebrite UFED prompts you to uninstall the client from the examined device.	Selected

Setting	Description	Default
Save extractions to	Sets a network location where extractions are saved. Tap **Browse** and enter the network location.	
Allow user predefined filter	Displays the timeframe and select parties windows during an extraction. This check box is not enabled by default. For more information on the User predefined filter, see User predefined filter (on page 32).	Selected
Enable extraction of deleted messages from SIM	Extracts deleted messages from a SIM. This check box is selected by default.	Selected
Require a password on wakeup	Requires the user to enter a password when Cellebrite UFED is in sleep mode.	Selected
Enable Android Backup APK Downgrade	Enables the Android Backup APK Downgrade method. This check box is selected by default.	Selected

Setting	Description	Default
Enable online device instructions	Displays the online device instructions instead of the offline device instructions. This check box is not enabled by default. This setting is for the Waiting for Device instructions, which explains how to connect a source device to Cellebrite UFED. If you have network performance issues when using the online device instructions, clear this check box.	Not selected
Show device restart alerts	Displays device restart alerts during the extraction process. This check box is not selected by default.	Not selected
Cable and Tip mode	Indicates the cable or tip to be used during the extraction.	Tip
Include Case details screen	Displays the Case details window during the extraction process. This check box is not enabled by default. For more information, see Case details (on page 31). If this check box is selected, you can also optionally display the extraction folder name according to the case details. The default is according to the device model name.	Not selected

Setting	Description	Default
Include camera screen	Displays the camera window during the extraction process. This check box is not enabled by default.	Not selected
Choose additional logo	Select an additional logo that will be displayed in the title bar of the home screen.	
Video quality	Set the video quality of the Cellebrite UFED camera to Best (1920 x 1280), Normal (1024 x 1280 default) or Low (640 x 480).	Normal
Enable device info (Advanced logical)	Displays the Device Info window during the Advanced Logical extraction. This window provides information on the device data, before performing an Android extraction.	Selected

7.1.1. Changing the application interface language

1. Tap the language field.
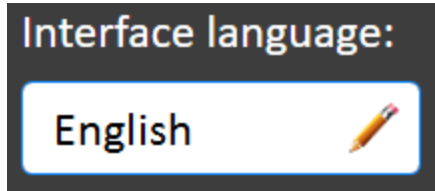
The Select Language screen appears with the current language selected. (In this case, **English**).
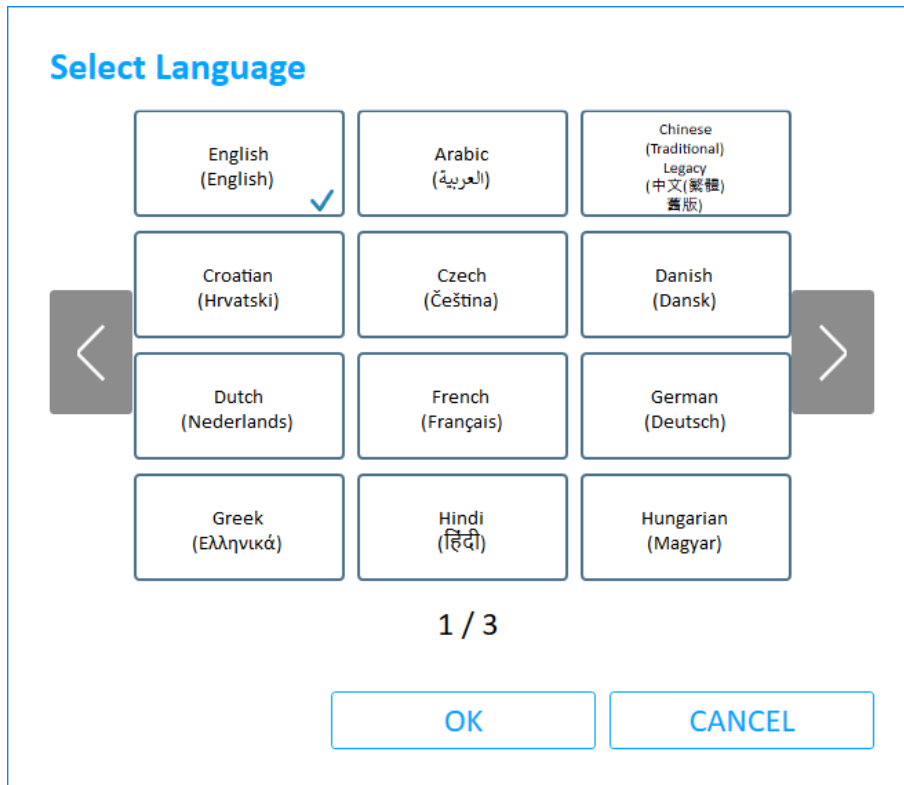
> Use the arrows to scroll through the list of available interface languages.

2. Tap the required language.
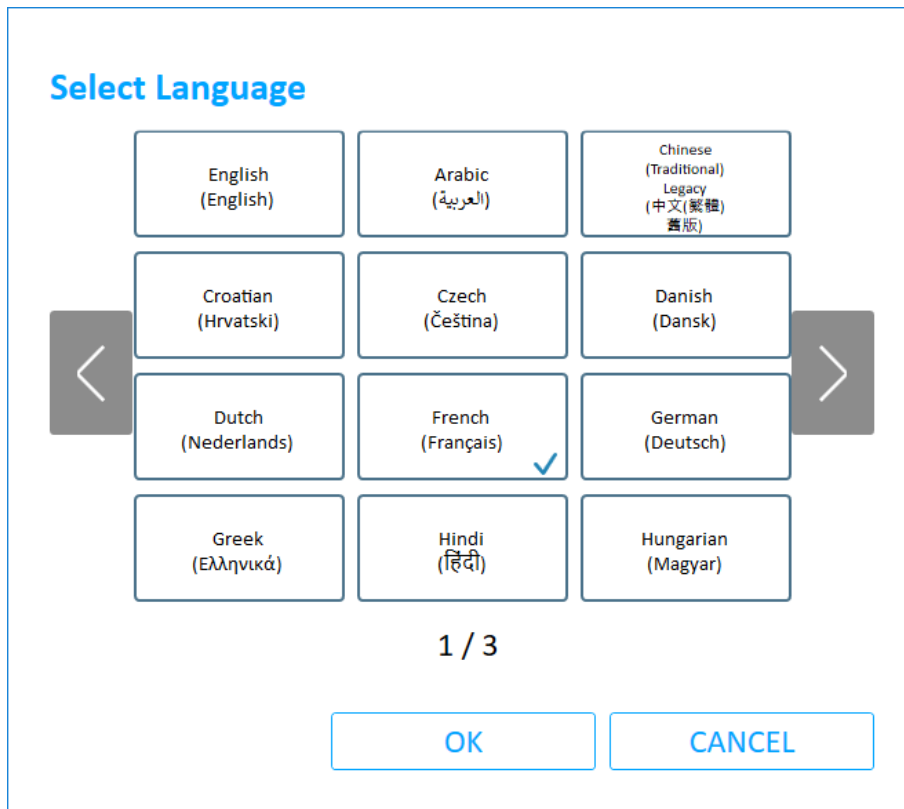
The following message appears (in the selected language):
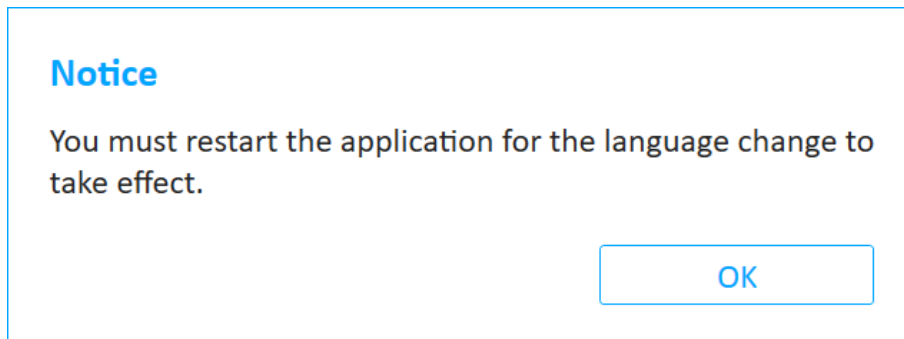
3. Tap **OK**.

   The **General** tab appears with the language of choice in the Interface language field.

4. Tap **Save** to close the Settings panel.

5. To restart the application:

   a. To close the application, tap in the application taskbar.

   b. To restart the application, do one of the following:

   » Tap the application shortcut icon located in the UFED shortcuts panel at the right of the screen.

   » Double-tap the Cellebrite UFED icon located on the Desktop.

» Tap **Start** > **Cellebrite UFED**

» Tap **Start** > **All Programs** > **Cellebrite Mobile Synchronization** > **Cellebrite UFED**.

Cellebrite UFED starts in the selected language.

> If Simplified Chinese is added to the Cellebrite UFED license, you will need to restart the application before the change will take effect.

7.2. Report settings

To set the report settings:

1. Access the **Settings** > **Reports** tab.

2. To set the generated reports language, tap ✏ next to **Generate Reports Language**, and select the desired language.

3. To set how the known issues notes about the extracted device are logged in the generated report, tap ⌄ next to **Note display modes**, and select one of the following:

   » **Disable** – Do not include device specific notes in the report.

   » **Separated Notes** – Add all the device specific notes at the end of the report.

   » **Embedded Notes** – Device-specific notes follow the content type they refer to in the report.

4. To set the generated reports visual formats, tap ⌄ next to **Report format**, and select one of the following:

   » **Normal** – The standard report structure, suitable to standard display screens.

   » **Compact** – A compact report structure, suitable for devices with a small display area.

5. To set the generated reports folder name formats, select ![icon] next to **Report folder format**, and select one of the following:

   » **Model Serial YYYY_MM_DD** – The folder name is constructed from <the model name> <the model serial> <the year in 4 digits>_<the month in 2 digits>_<the day in 2 digits>

   » **YYYYMMDD Model Serial** – The folder name is constructed from <the year in 4 digits><the month in 2 digits><the day in 2 digits> <the model name> <the model serial>

6. Select or clear **Hash using MD5** to toggle the display of the MD5 values which are generated for each file in the extracted data. This increases the time required to complete the extraction.

7. Select **Create MD5 list file** to generate a Checksums.md5 file that contains all the generated MD5 values of the extracted data.

8. Select or clear **Hash using SHA-256** to toggle the display of the SHA-256 values which are generated for each file in the extracted data.

9. Select or clear **Partial Extraction**, in the event of an extraction error, whether or not to include the partially extracted data up to the error point in the generated report.

10. Tap **Report custom fields** to add, remove and edit report fields. For more information, see Managing report fields (on the next page).

11. To set a field as required, tap the field in the **Required** column.

12. Tap **Save**.

7.2.1. Managing report fields

1. Tap **Report custom fields** to customize the report by defining additional fields which will be filled at the end of the extraction.

2. To add a new field:

   a. Tap **Add**.

   b. Enter the field name in the **Field Name** box.

> 📄 To display the keyboard, tap **Keyboard**.

   c. To set the field as mandatory, select **Required** next to the field name.

   d. Tap **Update**, or to exit without saving, tap **Cancel**.

3. To add additional fields, repeat step 2.

4. To edit an existing field:

   a. Tap the field in the list, and tap **Edit**.

   b. Repeat steps 2b-2d.

> 📄 You cannot edit the field name of a default custom field.

5. To delete a field:

a. Tap the field in the list, and tap **Delete**.

> ## Delete custom report field
>
> Are you sure you want to delete 'Notes' field?
>
> [YES]   [NO]

b. In the confirmation message, tap **Yes**.

6. Tap **Save** in the **Reports** tab.

7.3. System settings
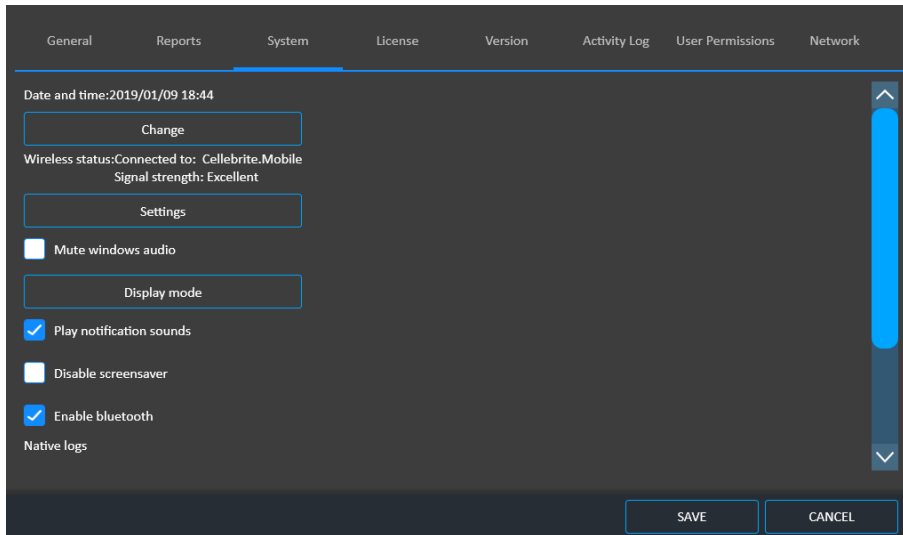
Define the following additional settings in the System tab:

» To change the date and time, tap **Change**.

» To set the wireless internet status, tap **Settings**.

» To change the appearance of the display, tap **Display mode**.

» To disable the audio system, select **Mute windows audio**.

» To set Cellebrite UFED to alert you when your attention is required, such as when it is waiting for your input or when an extraction fails, select **Play notification sounds**.

» To display the screensaver that appears after the unit is idle for a period, select **Disable screensaver**.

» To change the **ULG logs level**, select one of the following:

  » **Disabled** – The system will not generate log files.

  » **Detailed** – The system will generate detailed log files. The transaction will be slower in order to write to the log. Recommended in case of debugging/error situation.

> 📄 To save the ULG log files, connect a USB flash drive to a USB port at the back of the unit.

» To export system information, tap **Export system information**.

» To save the application logs, tap **Export application logs**.

» To update the App categorization DB to get insights from installed applications, go to **MyCellebrite > Products & licenses > Cellebrite UFED Touch 2 > Add-ons** to download the latest DB version. Unzip the DB file and click Browse to load the file.

» To monitor device usage, tap the **Extractions counter**. This counts the number of extractions performed by Cellebrite UFED. Transactions include all extractions per type and device tool actions. The counters are managed locally and can be reset.

> The password to reset the Extractions counter is the Computer ID or dongle serial number of the unit (displayed in the **License** tab).

7.4. License settings

The license can be updated via the network (Web), or a using an external device (via USB port).
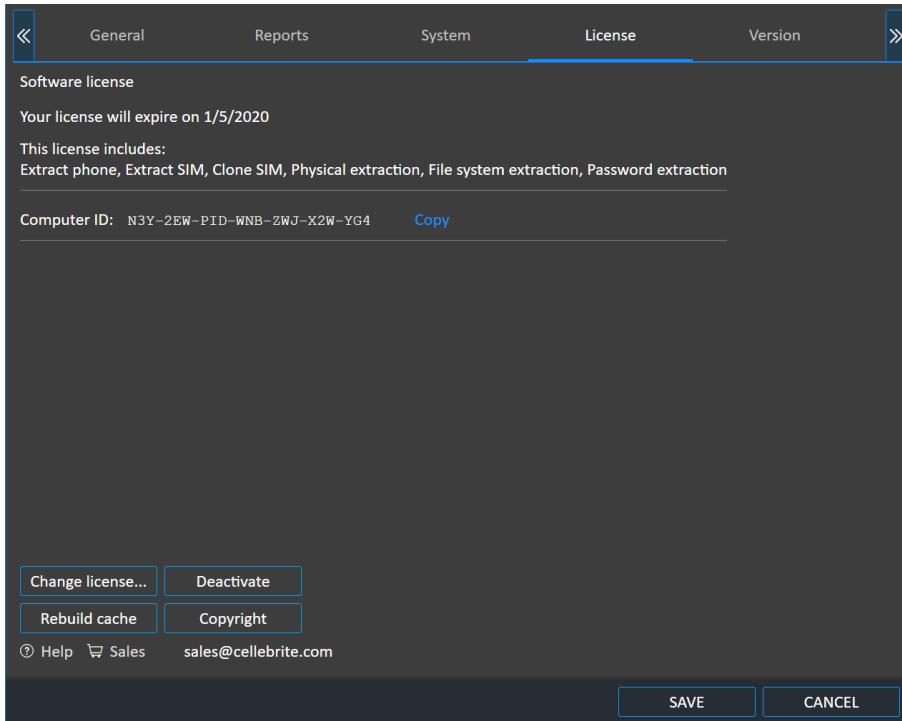
To update the license via the web:

> Before updating the license from the network ensure that the device is connected to the network.

1. In the **License** tab, tap **Change license.**
2. Select your license type.
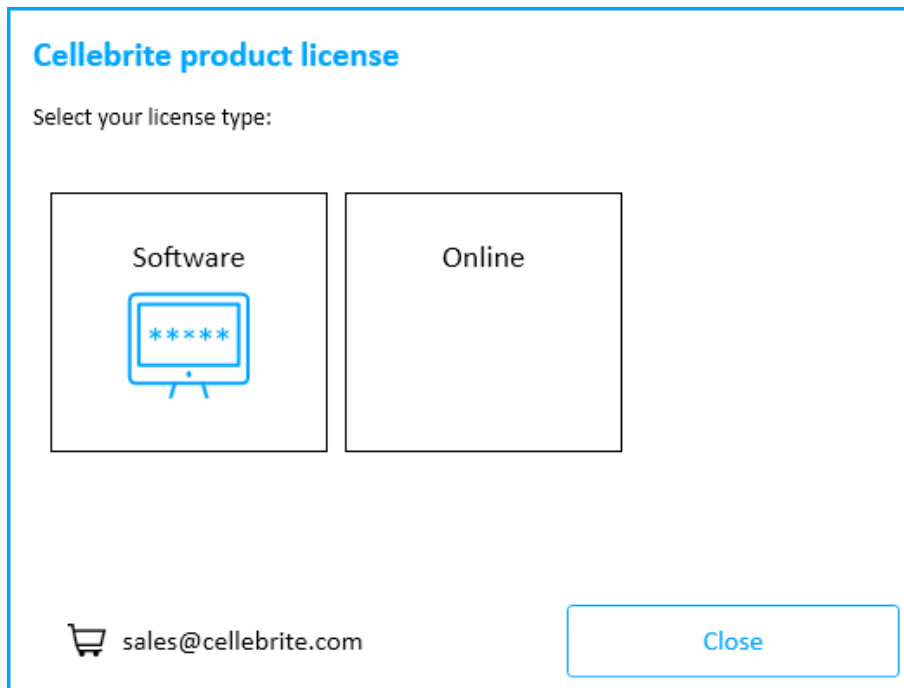
3. Tap **Accept** to accept the license agreement. The following screen appears.
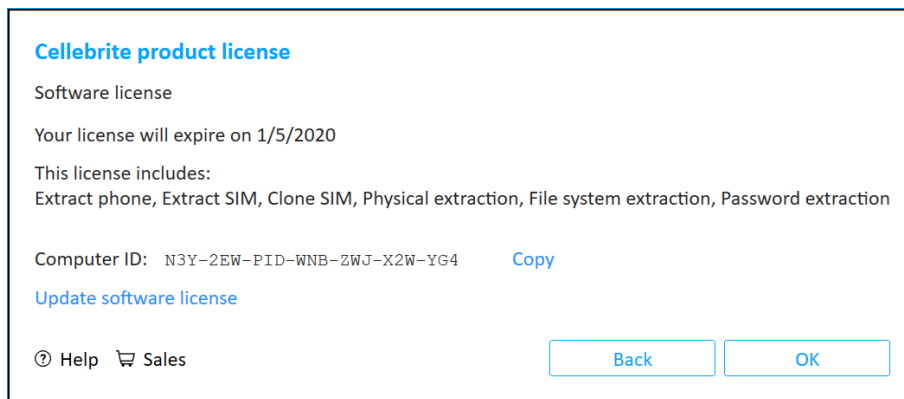
4. Tap **Update software license**. The following screen appears.

Cellebrite product license

Already have a license file?

Load license file

Load from the web

Need to download your software license?
Go to MyCellebrite

Computer ID: N3Y-2EW-PID-WNB-ZWJ-X2W-YG4   Copy

⑦ Help   🛒 Sales   Back   Close

5. Tap **Load from the Web**.

To update the license from an external device (via USB port):

1. Save the license file on the root directory of the USB flash drive.
2. Connect the external device to the Cellebrite UFED Ext1 or Ext 2 USB ports on the back panel.
3. In the **License** tab, tap **Change license**.
4. Tap **Accept** to accept the license agreement.
5. Tap **Update software license**.
6. Tap **Load license file**.

Cellebrite UFED identifies the license file automatically, and updated information appears on screen.

7.5. Version details

The version tab displays information about the Cellebrite UFED version and build.

Under Software updates, select the check box to automatically check for software updates.
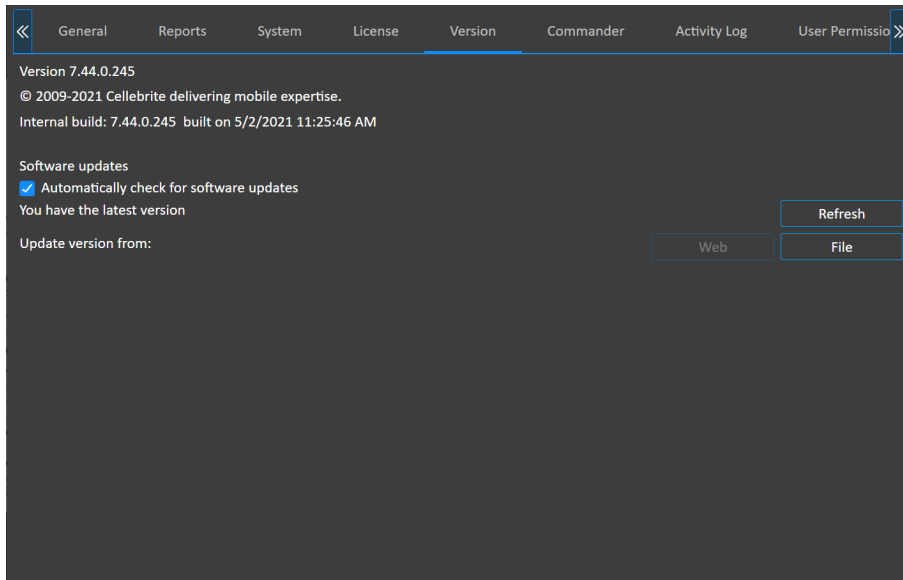
7.5.1. Connect a Cellebrite UFED device to Cellebrite Commander

Cellebrite UFED devices will automatically detect when a new Cellebrite Commander server is added to their subnet and prompt the user to connect automatically. If necessary, it is also possible to connect a Cellebrite UFED device to Cellebrite Commander manually.

> If more than one Cellebrite Commander is detected, the user can choose from the list of servers.

To connect a Cellebrite UFED device to Cellebrite Commander manually:

1. Go to **Settings** > **Commander**. The following window appears.
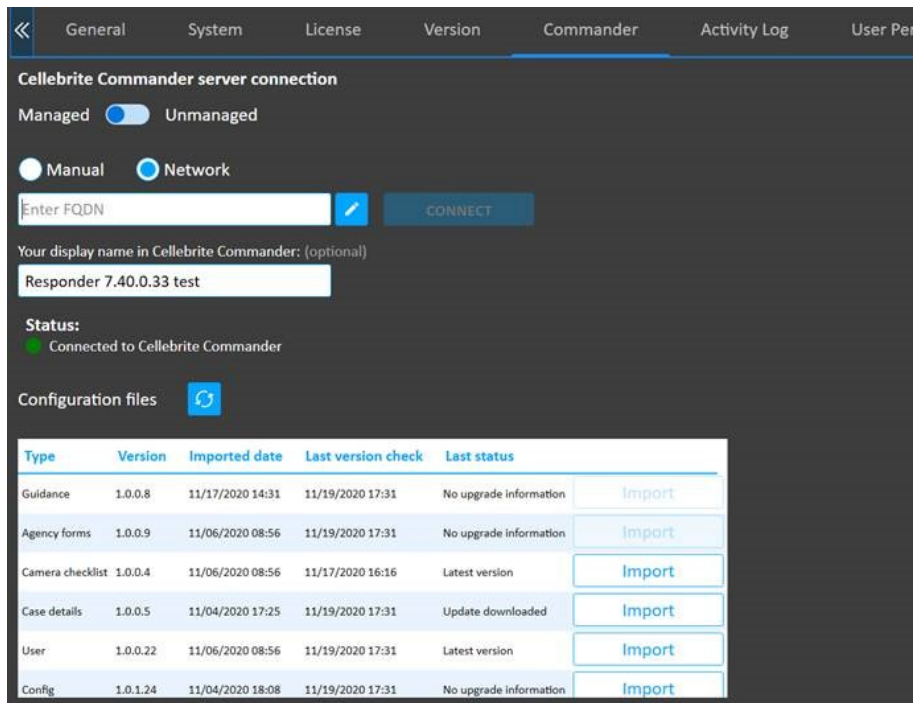
2. Select **Managed mode**.

3. Enter the FQDN (fully qualified domain name).

4. Tap **Connect**. If the validation is successful, the status changes to **Connected to Cellebrite Commander** .

5. Tap **Save**.

7.5.2. Updates and versions

When Cellebrite UFED is connected to the network, automatic notifications appear in the event of updates and new versions of the application.

» Tap **Refresh** in the Settings > **Version** tab to update the information available on the screen.

To install a newer version of the Cellebrite UFED application via the web:

> Before using this option, ensure that the unit is connected to the network.

» In the Settings > **Version** tab, in the **Version** area, tap **Web**.

The application is upgraded to the latest version available on the Cellebrite Commander (if relevant) or Cellebrite download server.

To install a newer version of the Cellebrite UFED application using an external device (via USB port):

1. Download the latest application version from your account in MyCellebrite, and save it to the root directory of the external device.
2. Connect the external device to the Cellebrite UFED Ext1 or Ext 2 USB ports on the back panel.
3. In the Settings > **Version** tab, in the **Version** area, tap **USB**.

   Cellebrite UFED identifies the new software file and starts the upgrade process.

7.5.3. Importing settings and configuration files

You can use Cellebrite Commander to download initial export files, which can then be edited if necessary and manually imported into Cellebrite UFED. These files can also be set using Cellebrite Commander. For more information, refer to the Cellebrite Commander manual.

Cellebrite UFED can import the following type of settings and configuration files:

» [Importing a camera checklist (on the facing page)](#)
» [Importing case details (on page 75)](#)
» [Importing user management (on page 77)](#)
» [Importing configuration files (on page 78)](#)

7.5.3.1. Importing a camera checklist

The camera checklist enables you to upload an XML file that the user can use as a reference as to what pictures are required of the device. As the user completes each step, they can place a check mark next to the completed items.

An example is displayed next.

To manually import a Camera checklist file:

1. In the **Version** tab, tap the **Import** button next to the setting file you would like to import. The following window appears.
2. Browse to the relevant file and tap **Open**.
3. Tap **OK** to update the application.

The following example shows the structure of the XML file.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<CheckListData>
      <Version>1.0.0.48</Version>
      <CheckListItems>
            <CheckListItem>Main screen</CheckListItem>
            <CheckListItem>Date and time</CheckListItem>
            <CheckListItem>IMEI number</CheckListItem>
      </CheckListItems>
</CheckListData>
```

7.5.3.2. Importing case details

You can import an XML file to change the options that appear in the Case Details window (see <u>Case details (on page 31)</u>).

To manually import a case details file:

1. In the Version tab, click the **Import** button next to the setting file you would like to import.
2. Browse to the relevant file and click **Open**.
3. Tap OK to update the application.

The following example shows the structure of the XML file.

```xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<CaseDetails>
    <Version>1.0.0.38</Version>
    <Fields>
        <Field>
            <Type>String</Type>
            <Caption>Case ID</Caption>
            <Mandatory>true</Mandatory>
            <AutoFill>true</AutoFill>
            <IsDefaultFolderName>true</IsDefaultFolderName>
        </Field>
        <Field>
            <Type>String</Type>
            <Caption>Seized by</Caption>
            <Mandatory>false</Mandatory>
            <AutoFill>false</AutoFill>
            <IsDefaultFolderName>false</IsDefaultFolderName>
        </Field>
        <Field>
            <Type>String</Type>
            <Caption>Crime type</Caption>
            <Mandatory>false</Mandatory>
            <AutoFill>false</AutoFill>
            <IsDefaultFolderName>false</IsDefaultFolderName>
            <Values>
                <Value>Armed Robbery</Value>
                <Value>Attempted Murder</Value>
                <Value>Child Exploitation</Value>
            </Values>
        </Field>
        <Field>
            <Type>String</Type>
            <Caption>Device owner</Caption>
            <Mandatory>false</Mandatory>
            <AutoFill>false</AutoFill>
            <IsDefaultFolderName>false</IsDefaultFolderName>
            <Values>
                <Value>Victim</Value>
                <Value>Suspect</Value>
                <Value>Witnesss</Value>
            </Values>
        </Field>
    </Fields>
</CaseDetails>
```

7.5.3.3. Importing user management

Cellebrite Commander enables user authentication ensuring that only users with the right credentials can access the application. Access rights are further enforced by defining permission levels per profile.

To manually import a user management file:

1. In the **Version** tab, select the **Import** button next to the setting file you would like to import.
2. Browse to the relevant file and tap **Open**.
3. Tap **OK** to update the application.

7.5.3.4. Importing configuration files

Configuration files enables you to import various settings into the system.

To manually import a configuration file:

1. In the **Version** tab, select the **Import** button next to the setting file you would like to import.
2. Browse to the relevant file and tap **Open**.
3. Tap **OK** to update the application.

7.6. Activity Log

The Activity Log lists all transactions performed by Cellebrite UFED. It includes information such as when the extraction started and ended, transaction type, duration, status, device vendor, device model, name, serial number of Cellebrite UFED, case ID, crime type, device owner, and who seized the device. You can also clear the activity log, export the activity data to a CSV file and show or hide the activity data.
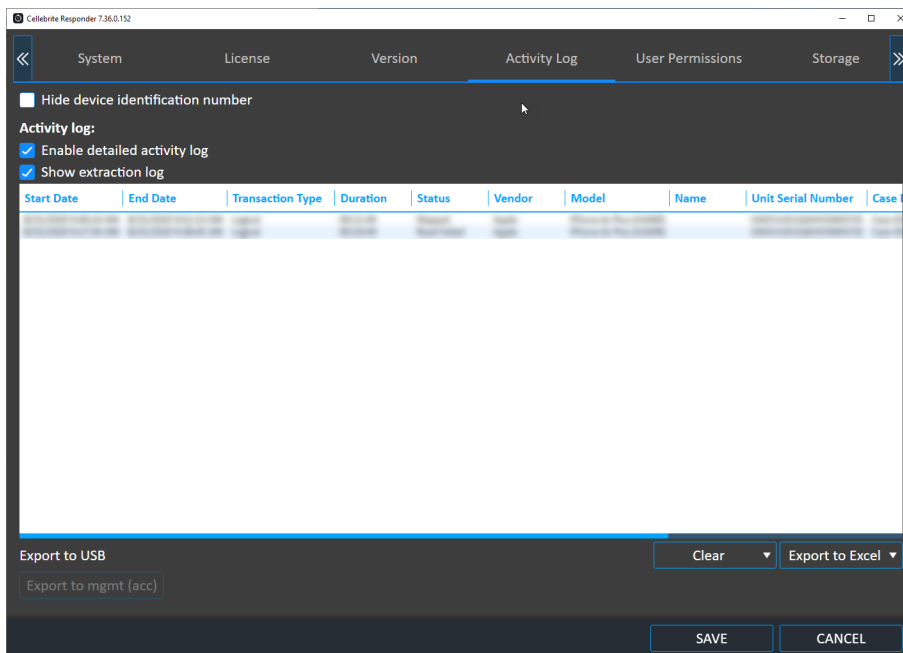
7.6.1. Exporting metadata to Cellebrite Commander

If a Cellebrite UFED unit is used in an offline environment, you can export the usage metadata file. This file contains the following: Cellebrite UFED device information (e.g., MAC address, serial number, software version number), transaction start times and end times, source phone information (e.g., vendor, model name, IMEI, and OS), and type of information extracted (e.g., Phone memory, SMS memory, MMS, pictures, videos, audio). The exported Zip file can then be manually imported into Cellebrite Commander. For more information, refer to the Cellebrite Commander manual.

To export the metadata:

1. Connect or reconnect a USB flash drive to the Cellebrite UFED unit. The button is only available when a USB drive is connected.
2. Tap the **Export to mgmt (acc)** button. The metadata can now be imported into Cellebrite Commander.

This button is only displayed if you are using the Managed mode (see Version details (on page 70)).

Exported data is removed from the Cellebrite UFED device and is not available for export again.

7.7. Users permissions

Define and configure user authentication settings to ensure that only users with the right credentials can access the application. Access rights are further enforced by defining permission levels per profile.

> User permissions can be set using Cellebrite Commander (refer to the Cellebrite Commander *manual*) or the UFED Permission Manager (see Permission management (on page 90)).
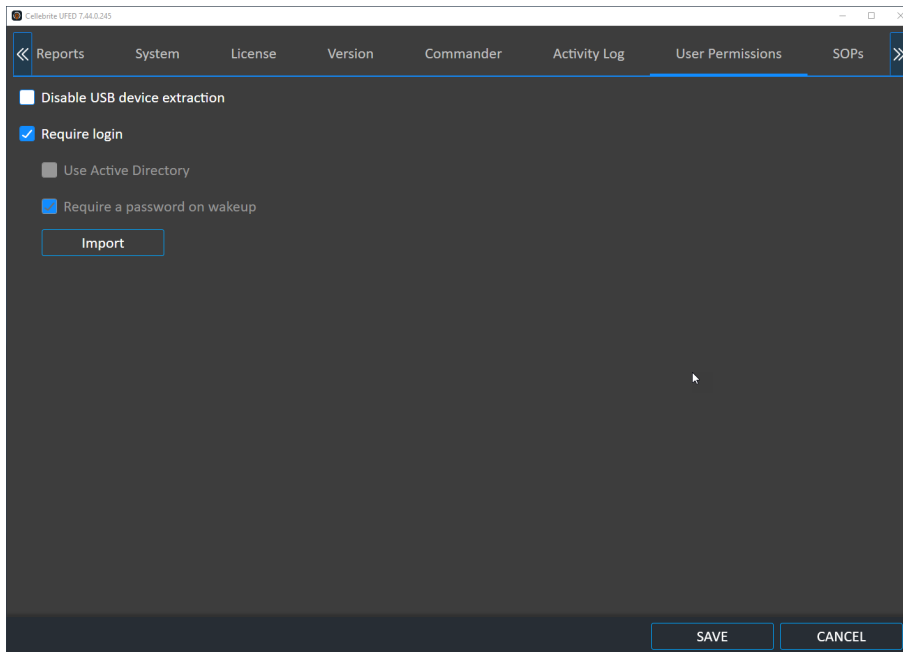
To disable USB device extraction:

» Select the **Disable USB device extraction** check box. The USB device option will not be available on the home screen.

To import user permissions:

1. Run the Cellebrite UFED as an administrator.
2. Click Import. The following warning appears.

3. Tap **Yes** and navigate to the directory where the permission management file (*.cp) is located. For information on creating a permission management file, see Using the Cellebrite UFED Permission Manager (on page 90).

4. Tap **Open** and then tap **Save**.

5. Restart the Cellebrite UFED application, which will now prompt for login credentials.

6. Use one of the login credentials configured in the permission management file. For more information, see Permission management (on page 90).

> Select the check box to require password on wakeup.

7.7.1. Active Directory integration

Active Directory is a Microsoft product providing a range of directory-based identity-related services. It authenticates and authorizes all users and computers in a Windows domain type network, assigning and enforcing security policies for all computers and installing or updating software.

When a user logs in to the system, Active Directory checks the submitted password and determines whether the user is a system administrator or normal user before allowing the user to log in. Active Directory also enables the management and storage of information at the admin level and provides authentication and authorization mechanisms.

Use the Windows Active Directory account to enable *quicker and easier* login to your Cellebrite UFED applications. Cellebrite UFED can manage the permissions with two permissions levels:

» Active Directory Groups
» Active Directory Users with Commander roles

7.7.1.1. Determining the Active Directory groups

> When using the **Groups level**, the permissions are applied according to the Active Directory groups of which the users are members (directly and indirectly). When using the **Users level**, you first need to map the users to Cellebrite Commander, and then to the permissions applied according to the selected profile in Cellebrite Commander. For more information, see To enable Active Directory (on page 85).

If required, use the following procedure to determine all the Active Directory groups for a specific user.

1. To get a list of groups for a specific user, replace the **USERNAME** with the actual user name

   Open up a command prompt (cmd.exe) and run:

```
gpresult /V /user USERNAME
```

2. The output will look like this (truncated with only the group info):

```
The user is a part of the following security groups

--------------------------------------------------

        Domain Users

        Everyone

        BUILTIN\Users

        NT AUTHORITY\INTERACTIVE

        CONSOLE LOGON

        NT AUTHORITY\Authenticated Users

        This Organization

        LOCAL

        Marketing

        Platforms Dev Team
```

> 📄 In the above example, you can see that this user is a member of several Active Directory (security) groups. In the following example we will use the "Platforms Dev Team" security group.

> 📄 If a group is contained within another group, other commands (such as `whoami /groups`) will only display the groups of which the user is a direct member. Therefore, it is recommended to avoid `whoami` as an indicator.

7.7.1.2. Using Cellebrite Commander

When using Cellebrite Commander, the system administrator needs to decide the permission management level. The possible levels are presented below:

Permission Level: Groups

Active Directory

Permission matched by Active Directory Group name to Profile name

CMS

Cannot set specific user permission

Permission Level: Users

Active Directory

Password validation

CMS

Permission is set by User's Profile
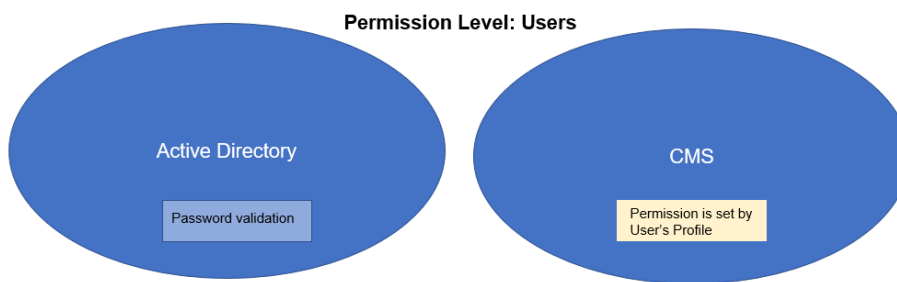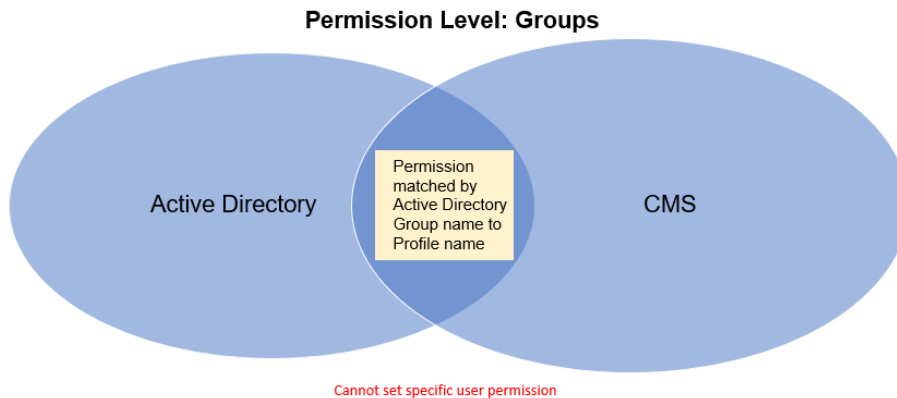
7.7.1.3. Initial setup

When Cellebrite Commander is used in conjunction with Active Directory, the following procedures are required for initial setup.

7.7.1.3.1. Permission Level – Groups

The Cellebrite Commander administrator needs to:

1. Create *profiles* with the exact same name of the relevant Active Directory groups.

2. Publish the users and permissions to all the relevant Cellebrite UFED units.

Once Active Directory is set up, each login request via a Windows user will be sent to Active Directory before approval. Active Directory checks the user's permissions and notifies the Cellebrite UFED unit whether to approve or deny the login request based on the user profile permissions.

> If the Cellebrite UFED units are offline, you will not be able to log in to the Cellebrite UFED unit. However, an ongoing session will not be disconnected if a disconnection occurred.

> Should you choose not to work with Active Directory, the Cellebrite Commander administrator can regulate the users and permissions via Cellebrite Commander or the Cellebrite UFED Permission Manager.

7.7.1.3.2. Permission Level – Users

The Cellebrite Commander administrator needs to:

1. Create *profiles* and set the permissions for each profile.
2. Import a CSV list of relevant *users* that matches the Users and Profiles settings in Cellebrite Commander.
3. Publish the users and permissions to all the relevant Cellebrite UFED units.

7.7.1.4. To enable Active Directory

1. In Cellebrite Commander select **Configurations > By product**. The following window appears.
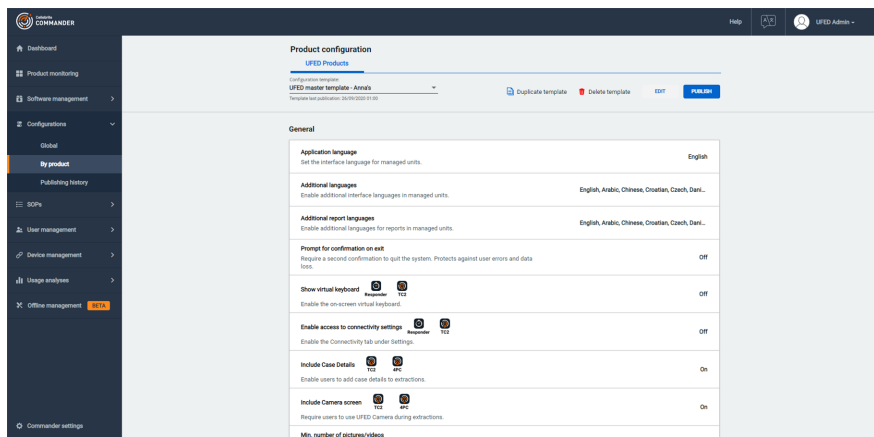
2. Click **Edit,**to enable the following under the Access Control section:

   a. **Require login**.

   b. **Enable Active Directory integration**.

3. Under **Permissions level**, select one of the following options:

   » **Active Directory groups:** Manage permissions at the Active Directory groups level. The match is performed by Active Directory group names.

   » **Active Directory users with Commander roles:** Manage permissions per user independently from Active Directory groups.

4. Click **Save** to save the configuration template.

5. Publish the configuration template to the relevant product.

Next you need to add the Active Directory profile and select the required permissions.

7.7.1.4.1. To add a role and select permissions

Adding roles and selecting permissions are managed in the User Management System. For more information, see the Managing Roles section in the User Management System manual.

7.7.1.4.2. Adding Users

Adding users is managed in the User Management System. For more information, see the Managing Users section in the User Management System manual.

7.7.1.5. Logging in to Cellebrite UFED

Once Active Directory is enabled, the following will occur depending on the Cellebrite UFED device you are using.

» In PC applications such as Cellebrite UFED 4PC and Cellebrite Responder, the login will occur automatically when you start the Cellebrite UFED application.

» In closed systems such as Cellebrite UFED Touch and Kiosk, Cellebrite UFED tries to locate the domain and display the following login screen.

1. Enter the Active Directory credentials.
2. Verify the Domain field.

> If the text in the "Domain" field (i.e., "domain controller host") is missing or incorrect, contact your IT department.

7.7.1.6. Cellebrite UFED Permission Manager

If you are not using Cellebrite Commander, use the following procedures in the Cellebrite UFED Permission Manager and Cellebrite UFED application to enable Active Directory.

To configure Active Directory in the Cellebrite UFED Permission Manager:

In the Cellebrite UFED Permission Manager, create a profile that corresponds to the required Active Directory group.

1. Run the Cellebrite UFED Permission Manager. The following window appears.
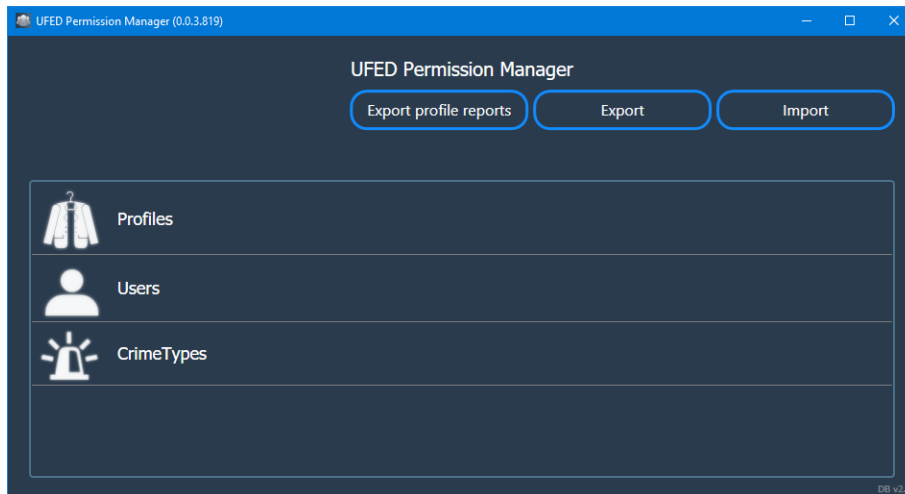
2. Click **Profiles** > **New Profile**. The following window appears.
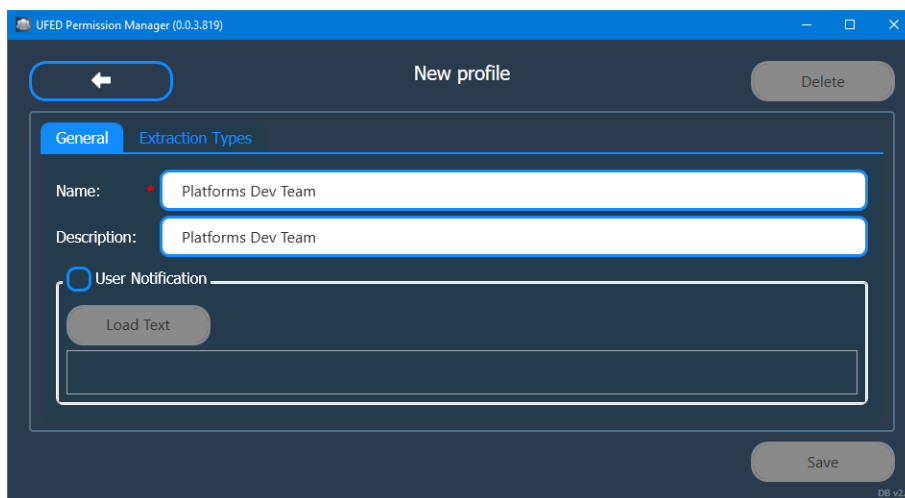
3. In the Name field enter the name of the Active Directory group. i.e., Platforms Dev Team.
4. Enter a description (optional).
5. Click **Extraction Types** and enter all the required permissions for the profile. The following window appears.
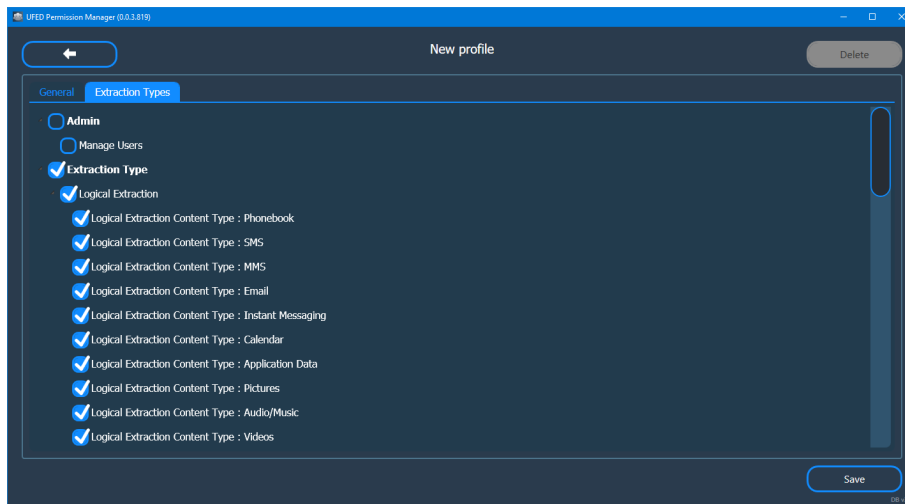
6. Click **Save**.

To enable Active Directory in the Cellebrite UFED application:

> 📄 This step is not required if you are using Cellebrite Commander.

1. In Cellebrite UFED go to **Settings** > **User Permissions**.
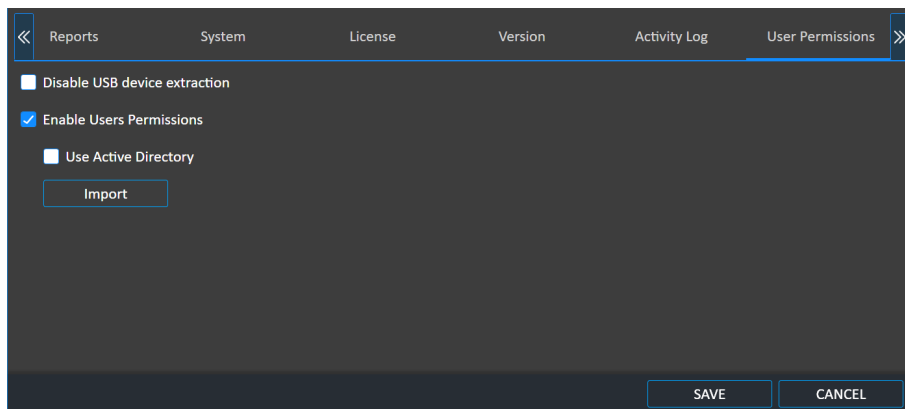
2. Select **Use Active Directory**.

> 📄 You can only login to the application using Active Directory users, there will no longer be Cellebrite UFED users such as Manager and Investigator. After activating Active Directory either in Cellebrite Commander or Cellebrite UFED application.

3. Click **Save**. The following window appears.

Notice

For the change to take effect, you must restart or log in to the application again.

OK

4. Click OK and restart the Cellebrite UFED application.

For information on how to login to the Cellebrite UFED devices, see Logging in to Cellebrite UFED (on page 87).

7.7.2. Permission management

Permission management can be performed via Cellebrite Commander or the Cellebrite UFED Permission Manager standalone application.

The Cellebrite UFED Permission Manager standalone application is available from MyCellebrite. Each profile contains access permissions, including operation rights per extraction type and content types. A single profile can be assigned to multiple users. The users and profiles can be exported into an encrypted permission management file, which can be imported into multiple Cellebrite UFED applications.

7.7.2.1. Using the Cellebrite UFED Permission Manager

To create a new profile:

1. Download the latest Cellebrite UFED Permission Manager application from your account in MyCellebrite, and save it to a directory on a computer or external device.
2. Run the Cellebrite UFED Permission Manager and follow the setup instructions. The Cellebrite UFED Permission Manager screen appears.
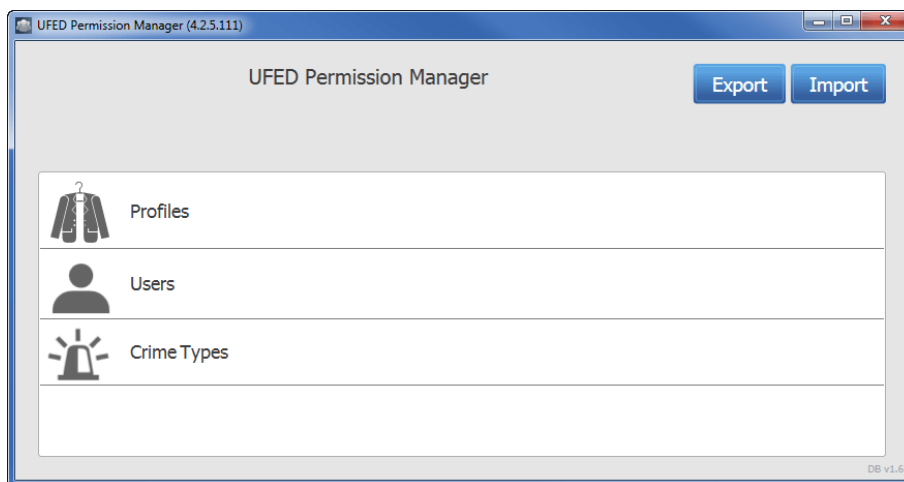
3. Tap **Profiles**.
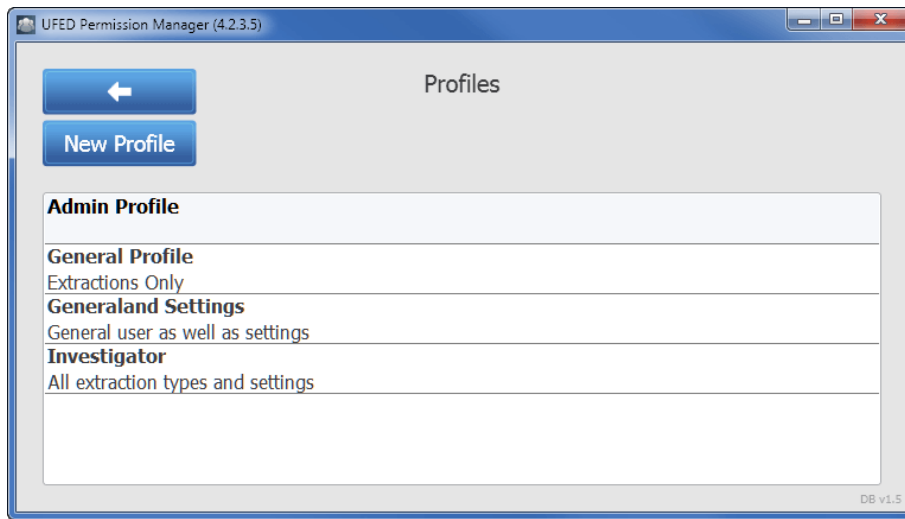
4. Tap **New Profile**. The following screen appears.
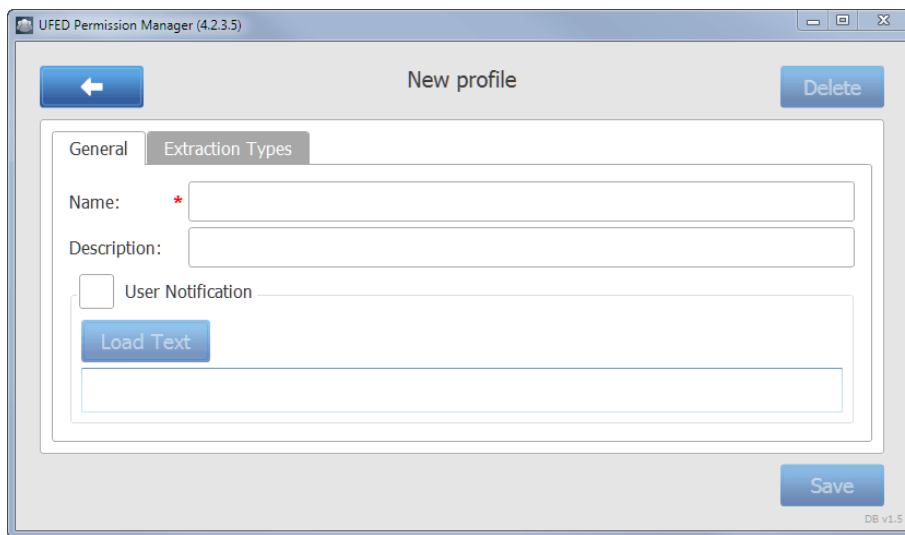
5. Enter a name and description for this profile.

6. If required select the **User Notification** check box, which enables you to load a RTF file with text and graphics for the profile.

7. Tap the **Extraction Types** tab.
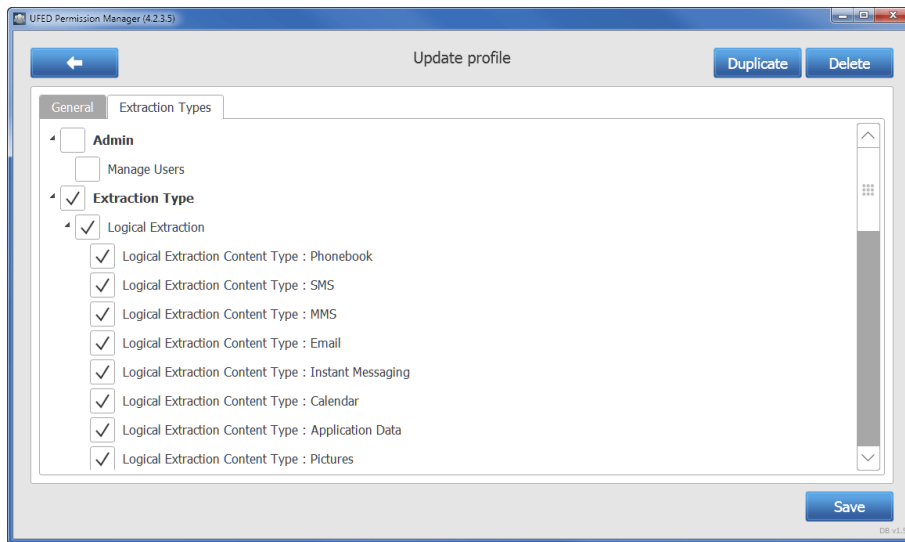
8. Select the options for this profile, such as Admin who can manage users, the Extraction Type (Logical Extraction, SIM Data extraction, Password extraction etc.) and UFED Settings (Activity Log).

> At least one of the enabled users must be an Administrator (Admin).

9. Tap **Save** and proceed to create a new user.

To create a new user:

1. In the Cellebrite UFED Permission Manager screen, tap **Users**. The following screen appears.
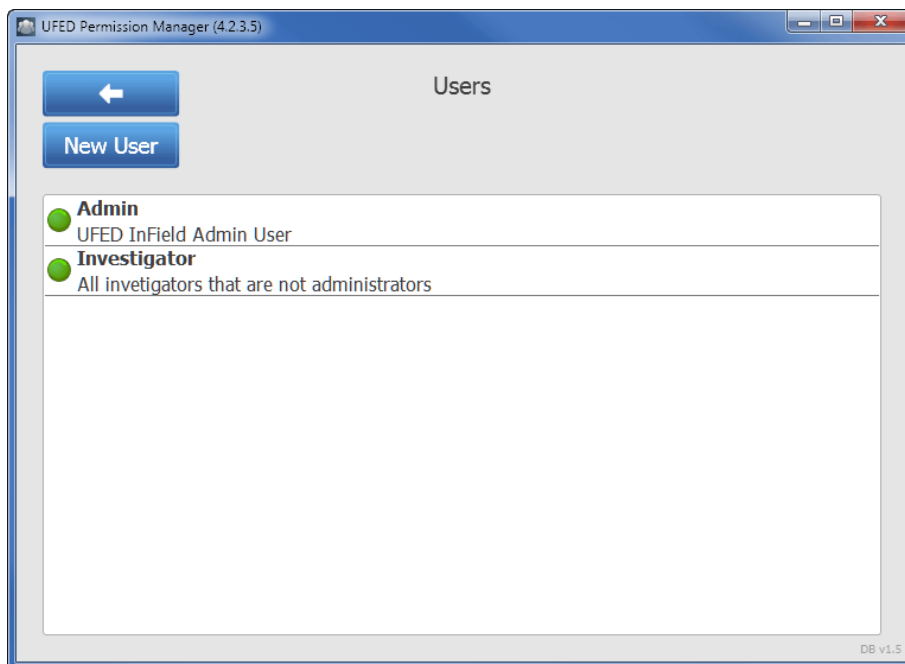
2. Tap **New User**. The following screen appears.

3. Enter the details for the new user including Username, Display Name, Description, and Password.

4. Select a profile for the user.

5. Select **Enabled** to enable the user.

6. Tap **Save**.

To manage crime types:

1. Tap **Crime Types**. The following screen appears.

> 📄 The crime types are only relevant for Cellebrite Responder.
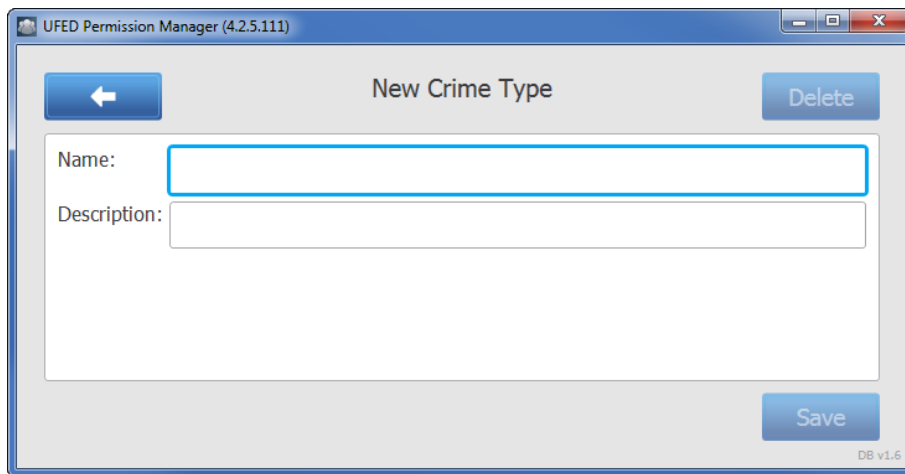
> 📄 You can delete all crime types; however you must add at least one crime to be able to export a permission management file.

> 📄 To edit a crime type, click the crime type and edit the Name.
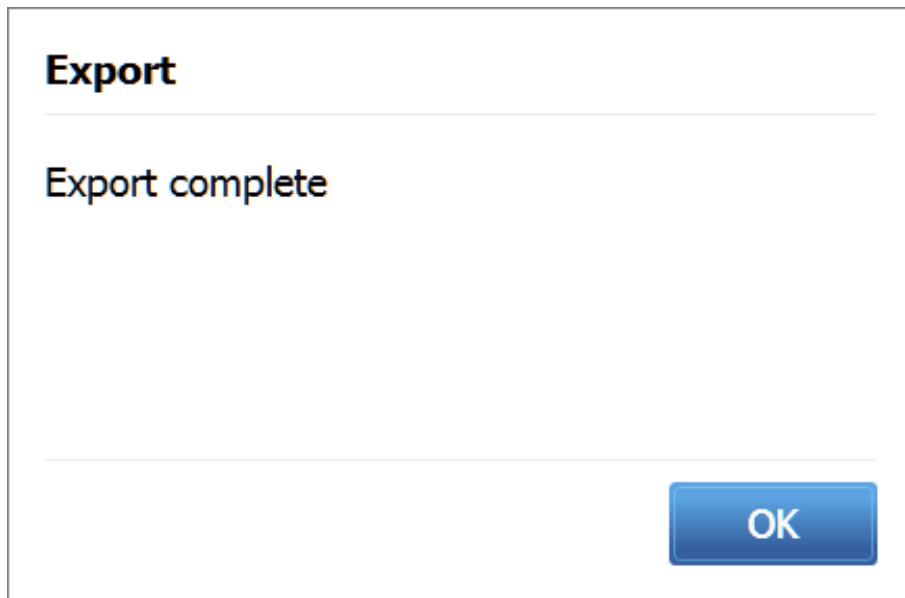
2. Tap **New Crime Type**. The following window appears.

3. Enter a name for the crime type and a description (optional).
4. Tap **Save**.

To export an encrypted permission management file:

1. In the Cellebrite UFED Permission Manager screen, tap **Export**, specify a directory for the file and tap **Save**. The following screen appears.

2. Tap OK. The permission file must be imported into Cellebrite UFED via the User Permissions tab in the Settings window.

> The next time you run the Cellebrite UFED Permission Manager you will be prompted for your user credentials to access the application.

7.8. Network

Local Area Network, Wireless Network Connection, Bluetooth Network Connection, and Proxy Server.

| General | Reports | System | License | Version | Activity Log | User Permissions | Network |

Ethernet

○ DHCP ○ Static

IP address: 192 . 168 . 56 . 95

Local Area Connection* 2

Subnet mask: 255 . 255 . 252 . 0

Default gateway: 192 . 168 . 59 . 254

Wi-Fi

Preferred DNS server: 192 . 168 . 100 . 26

Alternate DNS server: 192 . 168 . 100 . 20

Bluetooth Network Connection

Proxy Server

SAVE   CANCEL

8. Device tools

To access the device tools:

» From the Home screen, tap **Device tools**. The following window appears.

Activate TomTom trip log ⓘ	Android Debug Console ⓘ	Bluetooth scan ⓘ	Disable iTunes encryption password ⓘ
Exit Android Recovery Mode ⓘ	Exit Motorola Bootloop ⓘ	Exit Odin Mode ⓘ	Flash Cable 500 Firmware ⓘ
LG EDL recovery ⓘ	Nokia WP8 Recovery Tool ⓘ	Remove Android extraction files ⓘ	Switch to CDMA offline mode ⓘ
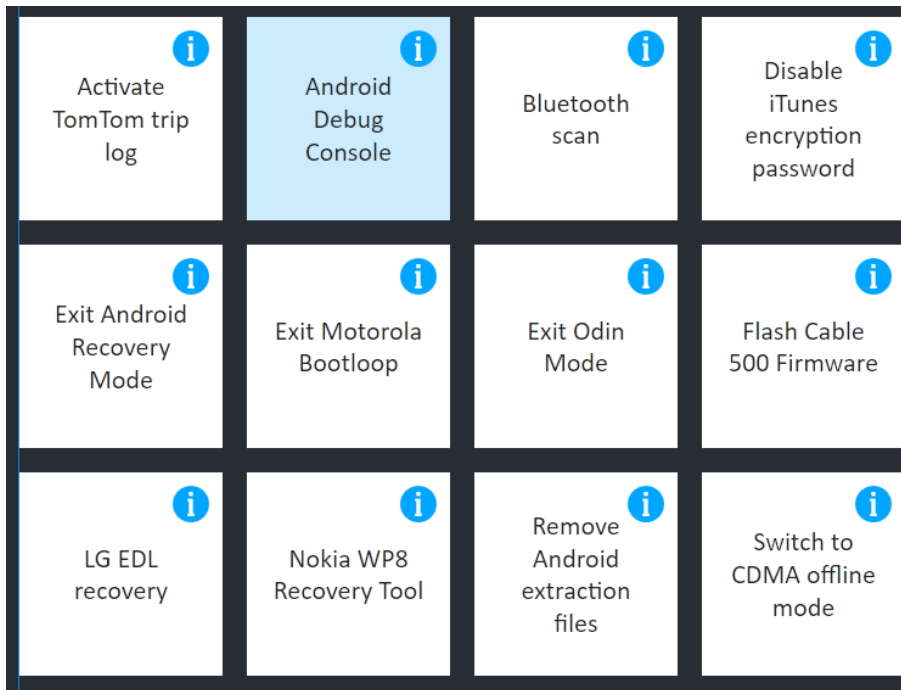
The **Device Tools** screen provides access to the following tools:

8.1. Activate TomTom trip log

This tool enables you to activate or deactivate the trip log logging feature of a connected TomTom device, which is often disabled by the user

To Activate TomTom trip log:

1. Tap **Tools** and then tap **Activate TomTom trip log**.

   The **Select Mode** prompt appears.

2. Select the desired mode.

   A prompt labeled **Attention** appears requesting to connect the device to Cellebrite UFED.

3. Connect the device to Cellebrite UFED.
4. Tap **Continue**.

8.2. Android Debug Console

This tool retrieves device information using Android Debug Bridge (ADB).

To use the tool:

1. Tap **Tools** and then tap **Android Debug Console**.
2. If required, you will be prompted to connect the Cellebrite UFED Device Adapter to a USB port (4PC and non-kiosk platforms only). The following window appears.

> **Device Tools**
>
> **Android Debug Console:**
> This tool uses Android Debug Bridge (ADB) and requires that the "USB Debugging" mode is enabled.
> To use this tool:
> 1. Go to the device settings > About/Information > tap the "Build number" 7 times. A message is displayed that you're now a developer.
> 2. Go back to the Developer options menu, select "USB debugging" and "Stay awake" (if available).
> 3. Approve the "Allow USB debugging" connection to the computer by selecting "Always allow".
>
> OK

3. Follow the on-screen instructions.
4. Tap **OK** to receive the device information. The following window appears.

Device Info

USB Descriptors

VID/PID	: 0x1004/0x633E
Manufacturer/Model	: LGE/LGL83BL
Interface 0	: MTP
Interface 1	: ADB Interface

ADB

Manufacturer/Model	: LGE/LGL83BL
Chipset	: Qualcomm Snapdragon 430

MSM8937 32 Bit

OS Version	: Android 7.0
Security Patch Version	: 2017-01-01
Encryption State	: encrypted
Rooted	: No
Battery Status (%)	: 90

REFRESH   OK

8.3. Bluetooth scan

This tool enables you to scan for available Bluetooth devices in your proximity and to pair with them. Make sure that Bluetooth is enabled on the device.

To perform a Bluetooth scan:

1. Tap **tools** and then tap **Bluetooth scan**.
2. Connect the Cellebrite UFED Device Adapter (4PC and non-kiosk platforms only).
3. A list of Bluetooth devices in the vicinity appears. Select one or the following options:
   » Tap one of the devices: The Device summary window appears.
   » Tap **Continue:** Device summary window appears
   » Tap **Refresh list:** Device tool in progress window appears and Cellebrite UFED tries to find additional devices.

Bluetooth Devices

| JBL T110BT | LGL83BL | POCOPHONE |

REFRESH LIST   CANCEL
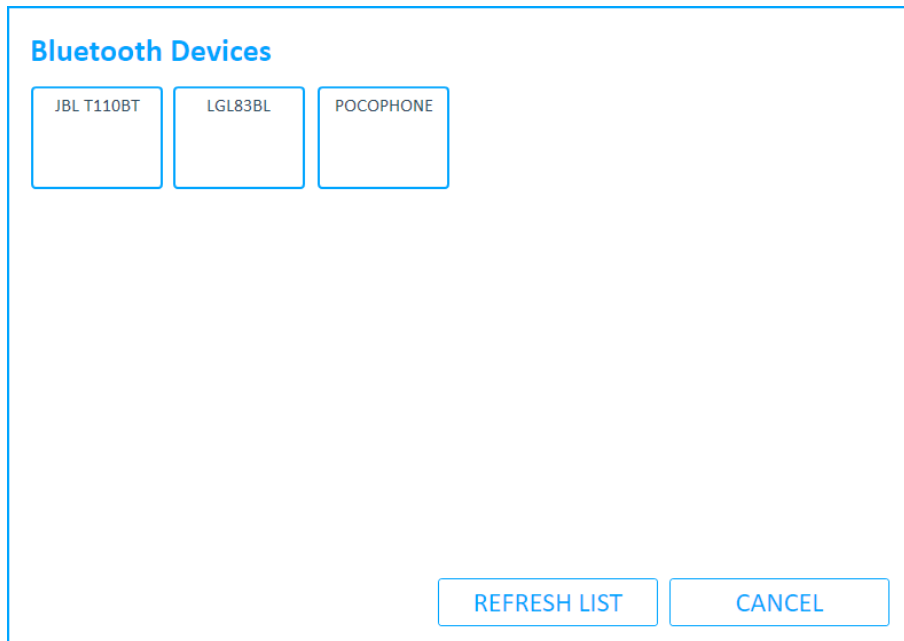
8.4. Disable iTunes encryption password

If you select to enable backup encryption during an iOS File system extraction (Full or Backup modes), and for any reason the extraction was stopped in the middle, the device may remain encrypted. This option resets the encryption on the device.

8.5. Exit Android recovery mode

This tool includes two options related to physical extractions using the Forensic Recovery Partition method on Android devices.

» **Exit recovery mode:** In some cases, due to device failure, or if the mobile device was improperly disconnected from Cellebrite UFED, the mobile device remains in recovery mode. This option enables the device to be taken out of recovery mode.

» **Exit bootloop:** In some cases, due to device failure, or if the mobile device was improperly disconnected from Cellebrite UFED, the mobile device keeps rebooting instead of entering the normal mode. This option enables the device to be taken out of this bootloop.

8.6. Exit Motorola Bootloop

In some cases, due to device failure, or if the Motorola mobile device was improperly disconnected from Cellebrite UFED, the mobile device keeps rebooting instead of entering the normal mode. This option enables the device to be taken out of this bootloop.

8.7. Exit Odin mode

To perform physical extractions on some Samsung devices, the device is placed in Odin mode. In some cases, due to device failure, or if the mobile device was improperly disconnected from Cellebrite UFED, the mobile device remains in Odin mode. This option enables the device to be taken out of Odin mode.

8.8. Flash Cable 500 Firmware

When using the Smart ADB method, the firmware on Cable No. 500 is changed and will no longer support the Cellebrite UFED User Lock Code Recovery Tool. The Flash Cable 500 Firmware tool flashes the required firmware to the cable to support either the Smart ADB method or the Cellebrite UFED User Lock Code Recovery Tool.

> In the Smart ADB method, Cellebrite UFED verifies the cable firmware and flashes it if required. Cellebrite UFED User Lock Code Recovery Tool does not include cable verification.

To flash the firmware for the Smart ADB extraction method:

1. Tap **Tools** and then tap **Flash Cable 500 Firmware**.
2. Connect the Cellebrite UFED Device Adapter to a USB port (4PC and non-kiosk platforms only).

3. Connect Cable No. 500 (side A) to the USB port.
4. Tap **Smart ADB Firmware** and wait for the process to finish.

8.9. LG EDL recovery

In some cases, due to device failure, or if the mobile device was improperly disconnected from Cellebrite UFED, the LG device remains in emergency download (EDL) mode and appears off. This option enables the device to be taken out of EDL mode.

To use the tool:

1. Tap **Tools** and then tap **LG EDL recovery**.
2. If required, you will be prompted to connect the Cellebrite UFED Device Adapter to a USB port (4PC and non-kiosk platforms only).
3. Follow the on-screen instructions.
4. Tap **Continue** and wait for the tool to finish running.

8.10. Nokia WP8 recovery tool

To perform physical extraction on some Nokia Windows Phone 8 devices, the device is placed in recovery mode. In some cases, due to device failure, or if the mobile device was improperly disconnected from Cellebrite UFED, the mobile device remains in recovery mode. This option enables the device to be taken out of recovery mode.

8.11. Remove Android extraction files

When performing extractions of devices with Android operating systems, a client is installed and some files are written to the mobile device. In some cases (e.g., due to a failure, or if the mobile device was improperly disconnected from Cellebrite UFED) the client and the files remain on the mobile device. This tool uninstalls the client and removes the files from the device.

8.12. Samsung Exynos Recovery

In some cases, due to device failure, or if the mobile device was improperly disconnected from Cellebrite UFED, the device remains off and the Android OS does not start. This option attempts to resolve this issue.

8.13. Switch to CDMA offline mode

This tool enables you to switch radio on CDMA devices to offline mode.

To switch to CDMA offline mode:

1. Tap **tools** and then tap **Switch to CDMA offline mode**.
2. Connect the Cellebrite UFED Device Adapter (4PC and non-kiosk platforms only). The Select Link prompt appears.

3. Select the link type (**USB Cable** or **Serial Cable**). The Device Tool in Progress window appears.
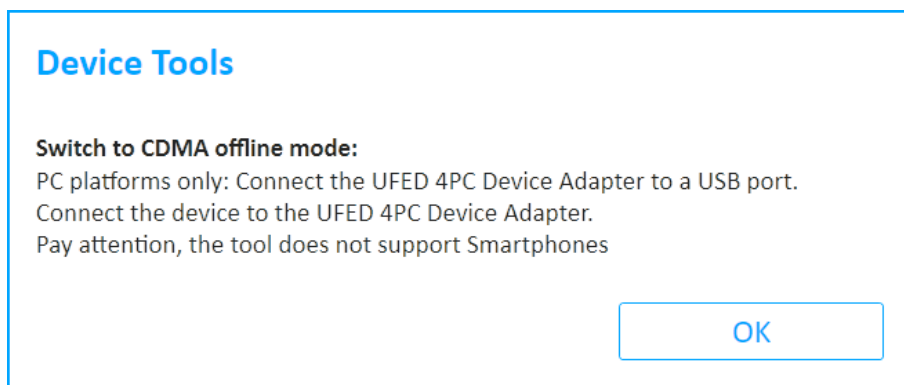
4. Tap OK.

   Upon completion, the Device Tool Summary appears.

8.14. Uninstall Windows mobile client

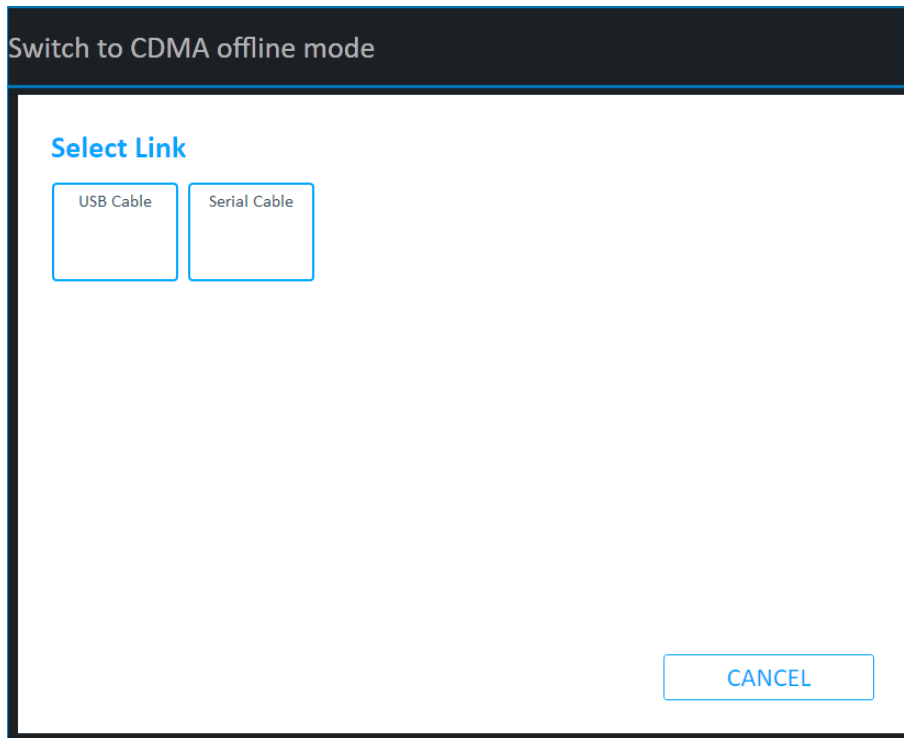To perform logical extractions on devices with Windows Phone operating systems, a client is installed on the device. In some cases, due to a device failure, or if the mobile device was improperly disconnected from Cellebrite UFED, the client remains installed on the mobile device. This option enables the client to be manually uninstalled.

9. Special cables

Cellebrite UFED requires special cables for certain functions. These include:

» The device power-up cable
» The U-441 Windows Easy Transfer Cable (used for the extraction to PC)

9.1. Device power-up cable

In case of a drained or absent battery, the device power-up cable powers the device instead of the battery while performing an extraction.

The device power-up cable contains four parts marked as: Data, Extra power, "-", "+".

Phone power-up cable

To connect the device power-up cable:

1. Connect the Extra Power connector to the Cellebrite UFED USB Port extension.
2. Connect the Data connector to the Cellebrite UFED USB Port extension.
3. Identify the device's battery contacts:
   » Open the device battery cover.
   » Locate the positive ('+') and negative ('–') pole markings of the battery, usually found next to the contacts area.
   » Make sure that the battery contacts are marked clearly on the device's body.
   » Remove the battery in order to gain access to the device's battery contacts.

   TIP: For battery contacts which are not clearly marked on the device's body, use the pole markings on the battery body to identify them. To do that, simply flip the battery along its contacts edge, and place it along the edge of the battery housing, then mark the device's contacts according to those on the battery.

> Use a multi-meter to identify the positive and negative poles of an unmarked battery.

4. Connect the **RED** alligator clip to the device's positive pole ('+'), the Primary **Black** alligator clip to the negative pole ('−') and the secondary **Black** alligator to middle pole in case of three poles or to the one next to the (-) in case of four poles. Make sure the alligator clips are not closing a circuit by touching each other.
5. Connect the source device to the **phone power-up cable** using the references cable from the cable organizer kit as listed in the Cellebrite UFED menu.

10. Technical specifications

> 📄 The specifications are subject to change without notice.

This section includes the following:

Battery (below)

Environmental (below)

General specifications (on the next page)

I/O interfaces (on page 109)

Kit weight and dimensions (on page 109)

Network (on page 110)

Power supply (on page 110)

Regulatory compliance (on page 111)

10.1. Battery

	Cellebrite UFEDStandard and Ruggedized
Type	Standard: Detachable 4 cells Li-Ion 18650 37 Wh
	Ruggedized: Detachable 4 cells Li-Ion 18650 46 Wh

10.2. Environmental

	Cellebrite UFED Standard and Ruggedized
	ETSI EN 300 019-1
Operating temperature	5° – +40 C, class 3.1
Storage temperature	-25° – +55° C, class 1.2
Transportation	-25° – +70° C, class 2.2 (in package only)
Humidity	5 – 85% not condensing
Shock/vibration (vehicle installation)	Part 1 -5, Class 5.1 and part1-7, Class 7.1

10.3. General specifications

	Cellebrite UFED Standard and Ruggedized
Display	Standard: LCD TFT, 7", WVGA 1024 x 600, 420 cd/m^2, 700 CR covered by SodaLime glass
	Ruggedized: LCD IPS, 7", WVGA 1024 x 600, 600 cd/m^2, 700 CR covered by GORILLA® GLASS 3
Operation system	Windows ® 10 IoT Enterprise 2015 LTSB for Small Tablets (ESD)
CPU	Intel ATOM 1.7 GHz and higher
Graphics specification	Intel® HD Graphics for Intel Atom® Processor
Memory	SODIMM DDR3L single channel Volume : 8GB Speed : 1600MHz
Storage	SATA2 M.2 SSD 128 GB[1]
Unit dimensions	223 mm (W) x 133 mm (D) x 61 mm (H)[2]
Weight	~780 grams
RF switch	Mechanical RF disable/enable slider switch
Recovery button	Rear panel tactile with backlight illumination button
Power button	Rear panel tactile with backlight illumination button
Touch panel	Capacitive, Multi-touch 5 points
Security	Kensington Lock
Cooling	Active by internal impeller
Case material	Coated plastic 50% ABS + 50% PC
Camera[3]	Resolution: 2592(H) x 1944(V), 5 MP

---

[1]Might change in the future.

[2]Without protection cover.

[3]Ruggedized

10.4. I/O interfaces

	Cellebrite UFED Standard and Ruggedized
USB ports	4 x USB 3.0 ports with 1.5A per port Target side: 1 Source side: 1 Rear panel: 2
Serial ports	Special serial port for feature phones connection on Source side only
SIM card reader	Build-in multi SIM reader including support for: SIM, Micro SIM, Nano SIM
SD card reader	Available card reader for: SD, SDHC, MMC, SDXC
Audio	HD CODEC based Realtek ALC886 chipset Stereo speakers 0.5W Built-in microphone Buzzer
Video Out	1 x Mini Display Port 1.3

10.5. Kit weight and dimensions

Weight & dimensions	Cellebrite UFED Standard	Cellebrite UFED Ruggedized
Case dimension (cm)	44 (L) x 33.5 (W) x 16 (H)	48.7(L) x 38.6 (W) x 18.5 (H)
Weight	6.5 Kg	10 Kg

10.6. Network

	Description
Wireless	Standard: WiFi: Dual Band with MIMO 1T1R technology IEEE 802.11 a/b/g/n/ac Bluetooth: Dual Mode 4.0/3.0
	Ruggadaized: WiFi: Dual Band with MIMO 2T2R technology IEEE 802.11 a/b/g/n/ac Bluetooth: Dual Mode 4.0/3.0
Ethernet	1 Gb Ethernet support based Intel LAN i210 chipset
Positioning	GPS + GLONASS[1]

10.7. Power supply

Part	Cellebrite UFED Standard and Ruggedized
Power supply	ACDC desktop adapter Input: 80 – 240VAC, 50 – 60Hz Output: 12V, 5A

---

[1]Various configurations, depends on costumer order.

10.8. Regulatory compliance

Part	Cellebrite UFED Standard and Ruggedized
CE This devise is in conformity with EU harmonization legislation.	
EMC	EN 301 489-1 EN 301 489-17 EN 61000-6-1 EN 61000-6-3 EN 55022
Safety	IEC/EN 60950-1 CB Scheme
Radio frequency spectrum usage	ETSI EN 300 328[1] ETSI EN 301 893
FCC	
EMC	FCC part 15, subpart B
Radio	FCC part15.247 FCC part15.407

[1]Provided by OEM RF module.

11. Battery replacement procedure

> CAUTION: There is a danger of explosion if the battery is replaced incorrectly.
> Replace only with the same or equivalent type recommended by the manufacturer.
> Before disposing the battery, make sure it is fully discharged.
> Discard used batteries according to regulation in your country.

11.1. Introduction

This section describes the Cellebrite UFED battery replacement procedure.

The Cellebrite battery replacement kit is provided to Cellebrite customers and partners. Replacing Cellebrite UFED battery does not require high proficiency level, however strict following of the procedures in their correct order is mandatory.

Improper operation of the battery replacement procedure, may cause damage to the Cellebrite Cellebrite UFED unit. Read this document before you start, follow the procedures and instructions carefully.

11.1.1. Battery replacement kit Contents

The Cellebrite battery replacement kit contains the following:

» Sanyo Li-Ion battery pack.

11.2. Replacing the battery

» There is a danger of explosion if the battery is replaced incorrectly.
» Replace only with the same or equivalent type recommended by the manufacturer. Removing the old battery:

> Shut down the system before replacing the battery.

1. Disconnect the Cellebrite Cellebrite UFED unit from the external power supply.
2. Make sure that the Cellebrite UFED is in power off mode.
3. Battery removal - Unscrew the screw closing the battery assembly.
4. Remove the battery assembly by lifting the notch.

Figure 1: Cellebrite UFED bottom view with battery installed

Notch for panel lifting

Battery panel screw

Figure 2: Battery notch view

Figure 3: Removed battery view

Figure 4: Battery label view

Figure 5: Battery connector view

11.3. Installing the new battery

1. Hold the battery assembly with connector facing the battery mating connector of Cellebrite UFED.
2. Insert the battery assembly into its mating connector.
3. Press slightly the whole assembly, verify it fits firmly in the dedicated location.
4. Secure the assembly with the screw.
5. Turn Power On switch, verify that Cellebrite UFED turns on.
6. Connect the external DC power supply.

> Before disposing the battery, make sure it is fully discharged.
> Discard used batteries according to regulation in your country.
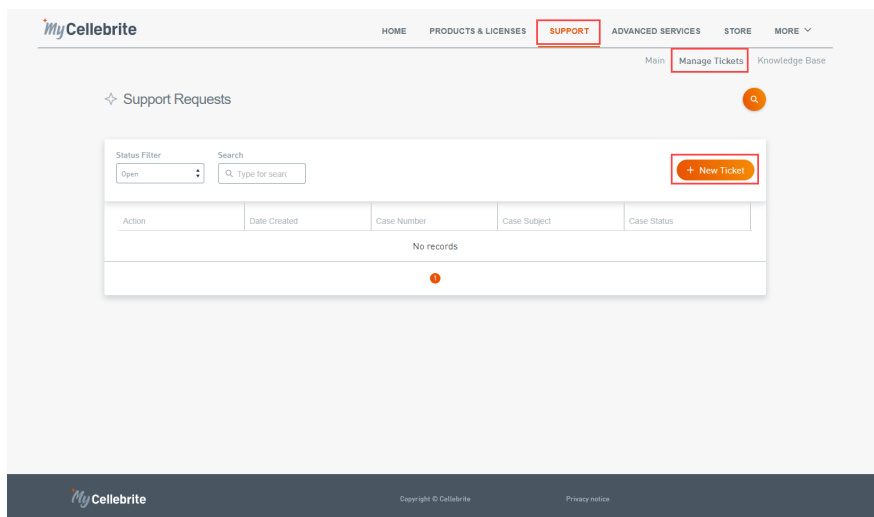
12. Ordering cables and accessories

If you have a valid Cellebrite UFED Touch license, it is possible to request missing cables and accessories in the MyCellebrite portal.

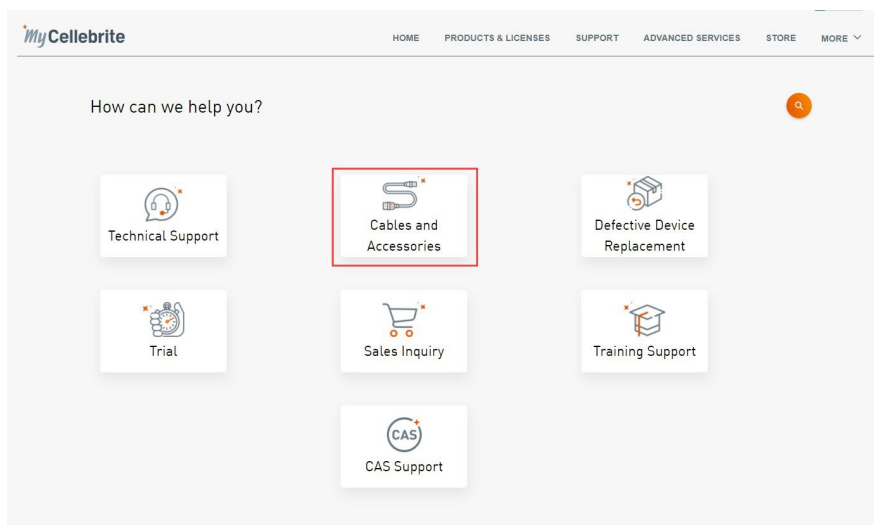Customers can request up to two cables from each cable type per year at no charge.

Once ordered, you will receive a confirmation that your request has been accepted, and a notification when shipped.

To order cables and accessories:
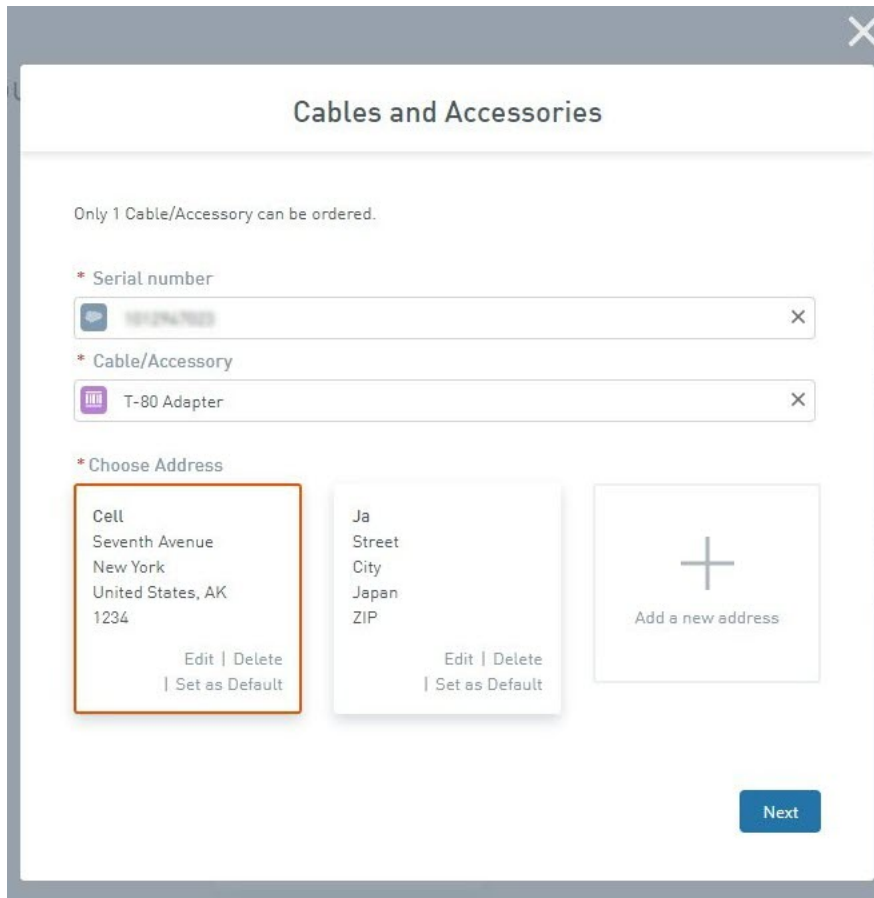
1. Go to the MyCellebrite portal.
2. Navigate to **Support > Manage Tickets**.
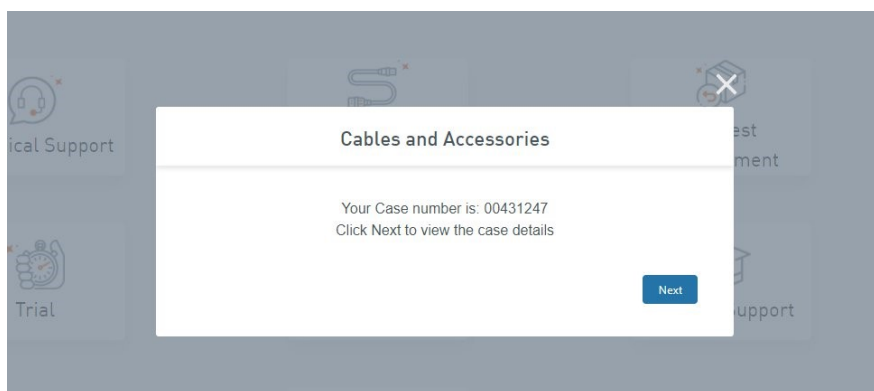3. Click **+ New Ticket**.

4. Click **Cables & Accessories**.

5. Enter the serial number for the product.

6. Select the cable or accessory.

7. Select or add a new address.

8. Click **Next**.

9. Click **Next.**

10. The case details are displayed.

11. Once the cables are shipped you will receive an email notification with the tracking number.

12. You can view the case and its status any time in the MyCellebrite portal by going to **Support > Manage Tickets:**

13. Glossary

A

Active extension cable

This cable is 150 cm in length and allows for the easy and accessible placement of the UFED Device Adapter with USB 3.0.

ADB

Refers to an extraction method most commonly used for file system extractions. ADB, AKA Android Debug Bridge, is a built-in communication mechanism originally designed for device debugging. To enable the device extraction, ADB must be turned on.

ADB (Rooted)

When extracting a rooted device, the operating system version is not a limitation and the extraction can be completed on any Android version.

Advanced ADB

Refers to a physical extraction method, where ADB is used to facilitate the extraction. This method is available for Android OS versions created before December 2016. Depending on the device, this extraction may perform faster than other extraction methods, but takes considerably longer than other extraction methods. With this extraction type, the source device will continue the extraction, once the appropriate commands are sent to the device, with the output directed towards a USB mass storage device (via OTG cable) or SD memory card.

Advanced ADB (Generic)

This process is similar to the ADVANCED ADB mentioned however it is not verified for use on a specific device. It has however been shown to be successful on many

similar devices. In some rare cases, it may not perform as expected, therefore, we recommend trying other extraction types first.

Advanced logical extraction

An extraction method that combines both the logical and file system extractions into a single extraction method. This method helps users overcome the pain of long and convoluted extractions, saving time and effort while maintaining forensically sound data.

Airplane mode

Flight mode, Offline mode, or Standalone mode is a setting that when activated it disables all voice, text, telephone, and other signal-transmitting technologies such as Wi-Fi and Bluetooth. Wi-Fi and Bluetooth can be enabled separately even while the device is in airplane mode.

Allocated space

The area on a device's memory that stores data in an organized manner, and contains its operating system and user data. Logical extractions obtain data from allocated space only.

Android Backup

Supports Android devices running OS version 4.1 and later. It typically provides less data than a regular "ADB" backup, however, depending on the make, model and OS version of the device, it may be the only option available or can be used when the ADB option exists, but is not successful.

Android Backup APK Downgrade extraction

This method focuses on specifically supported apps for decoding. It should be used as a last resort method as data alteration will occur during this process. This method temporarily downgrades the updated version of the app on the device and installs the latest supported version of the app that it can decode.

Cellebrite

apk

Android application package file. Each Android application is compiled and packaged in a single file that includes all of the application's code (.dex files), resources, assets, and manifest file.

Apple File Conduit

AFC2. A service that is used by computer applications such as iTunes and iPhoto to read files from a device over USB.

B

Boot loader

A small piece of code that is inserted into the RAM during start-up. In the commercial wireless world, this allows flashing of firmware. In the forensic world, it allows a non-intrusive means of accessing and copying user data into a forensic image.

Brick

A device that cannot function in any capacity (such as a device with damaged firmware).

Bruteforce

Refers to an unlocking technique that relies on trial and error. Combinations are attempted until the correct password or PIN is found.

C

CAS

Cellebrite Advanced Services (CAS) offers customers the ability to recover valuable evidence from heavily damaged, locked or encrypted devices.

CDMA

Code Division Multiple Access. These networks connect using different methods to allow multiple callers access to single voice radio waves, hence Code and Time Division. True CDMA networks do not require handsets to have a SIM card, as the network connects to the device and the subscriber details are contained in the handset rather than a SIM card.

Cellebrite Commander

Simplify how you manage and control all deployed devices and systems with the Cellebrite Commander. Reduce ongoing administration costs by remotely accessing devices and systems across your operation.

Cellebrite UFED 4PC

Enables users to deploy extraction capabilities on Windows based tablets, laptops, and desktop computer systems. It performs physical, logical, file system and password extractions on a wide range of devices.

Cellebrite UFED Touch

Enables the simplified extraction of mobile device data. Depending on the license purchased, it performs physical, logical, file system and password extractions on a wide range of devices.

Chip-off

Otain data straight from the mobile device's memory chip.The chip is detached from the device and a chip reader or a second device is used to extract data stored on the device under investigation.

Client

A client is used during some extractions (usually Logical extraction). It is a very small application that is temporarily installed on a limited number of Android, older Windows Mobile, Palm OS, and Symbian models. The client is unlike a boot loader in that, rather than be installed to the device RAM, it acts like any other third-party app

by installing to the device ROM. It does not overwrite any data; it will not install, for example, on a device whose memory is full. It provides enough access to the device's file system that allows UFED to index the file system and determine how many files exist, then extract the data. It is automatically removed from the device afterthe extraction completes. Users are encouraged to document when the UFED prompts them to use the client, and whether they proceed with the extraction.

D

Decrypting Bootloader

This process is designed for Android devices that have Qualcomm chipsets. This extraction can be performed when the device is in Bootloader mode. Bootloader extractions do not support extractions from a memory card or SIM card.

Device power-up cable

In case of a drained or absent battery, the device power-up cable powers the device instead of the battery while performing an extraction. The device power-up cable contains four parts marked as: Data, Extra power, "-", "+".

E

EDL (Emergency Download)

Included in the cable or tip set received with your UFED, is an EDL cable. The EDL method is sometimes a superior alternative to advanced techniques, such as JTAG, ISP and Chip-off as they typically can be accomplished without advanced or invasive techniques. It's also possible to use this method on devices that do not function due to damage.

Extraction

The process of obtaining mobile device data and storing it in an approved location for processing.

Extraction files

Files used to capture forensic evidence from mobile devices. This includes mobile phones, handheld tablets, portable GPS devices, and devices manufactured with Chinese chipsets. Extraction types include Logical, SIM Password, File system, physical, capture images, and capture screen shots. Extraction files: MSAB Extended XML, XLS, XLSX, XMK, CSV, TXT, UFD, UFDR, CDR

F

Facelock

Uses an image of the user captured by the front camera to unlock the device. There must be some movement in the face when unlocking the device, to prevent someone from using a still photo to gain access.

File system extraction

Obtains files embedded in the memory of a mobile device. Retrieve the artifacts within a Logical extraction, in addition to hidden system files, databases and other files which were not visible within a logical extraction.

Fingerprint

Newer devices have a fingerprint sensor built into the home button. The user places their finger upon the sensor to gain access to the device.

Forensic Recovery Partition

This extraction method will perform a physical extraction while the device is in Recovery mode. With this extraction method, the original recovery partition is replaced with Cellebrite's custom forensic recovery partition. Using Cellebrite's custom forensic recovery partition does not affect any of the user data, is forensically sound, and will bypass the user lock from a number of Samsung Android devices.

 Cellebrite

Forensically sound

Extracted data is said to be forensically sound if it was collected, analyzed, handled, and stored in a manner that is acceptable by the law, and there is reasonable evidence to prove so. Forensic soundness provides reasonable assurance that extracted data was not corrupted or destroyed during investigative processes, whether on purpose or by accident.

I

ICCID

Integrated Circuit Card Identifier. GSM identifier

IMEI

International Mobile Equipment Identifier. GSM identifier

IMSI

International Mobile Subscriber Identity. GSM identifier

Iris scan

Different from retina scans, an iris scan is a form of biometric identification using iris pattern-recognition techniques. The owner of the device establishes the security feature by video scanning the complex, unique but stable patterns of the eye portion surrounding the pupil.

J

Jailbreaking

A jailbroken iOS device or a rooted Android device is one whose owner has taken steps to bypass its factory settings, including built-in security and other restrictions. Jailbreaking an iOS device allows the user to install third-party apps from sources other than the App Store, while rooting an Android device provides administrative "root" access to its operating system. UFED solutions do not rely on jailbreaking or

permanent rooting to perform forensic extractions, as other mobile forensic tools do.

K

Knock pattern

The user taps certain locations on the screen in a certain order to gain access to the device.

L

Logical extraction

Extracts user data from a mobile device (SMS, call logs, pictures, phonebook, videos, audio, certain application data, and more). Quickest extraction method but least amount of data.

M

MEID

Mobile Equipment Identity (MEID) is the CDMA equivalent of the International Mobile Equipment Identifier (IMEI) for Global System for Mobile communications (GSM) handsets and is often referred to as the serial number of the handset.

MIN

Mobile ID Number (MIN) is often compared to the International Mobile Subscriber Identity (IMSI) found associated to GSM handsets. The MIN is the number which identifies the subscriber to the CDMA network provider.

MSISDN

Mobile Station International Subscriber Dialing Number. GSM identifier.

Cellebrite

MultiSIM Adapter

Is a small-size adaptor which enables reading, data extraction and cloning Nano SIM, Micro SIM and SIM cards.

P

Password Lock/Bypass

Users of devices are routinely secure their data with the user of password locks and security measures. The bypassing or discovery of these security measures largely depends on the make and model of the device as well as the operating system that is in use. Using Cellebrite's extraction technology, some devices are able to have bypasses, where a series of specialized cables and instructions are supplied to either bypass or defeat a security mechanism used. In other cases, instructions will be provided which will allow the user to have the PIN/PASSCODE displayed on the screen.

Physical extraction

The most comprehensive extraction and forensically sound. It uses advanced methods to extract a physical bit-for-bit image of the flash memory of a device, including the unallocated space. Unallocated space is the area of the flash memory that is no longer tracked by the file system. Unallocated space may contain images, videos, files, and more.

Physical/Logical Analyzer

An analysis and reporting tool for logical, file system and physical extractions. This software solution provides users with the capability to extract data, perform advanced analysis, decoding and reporting and presenting the results in a clear and concise manner.

PIN/Password and Pattern Lock

All of the above locks require a secondary lock such as a PIN, password, or pattern lock. Also, a user may select one of these as the primary screen lock for their device.

R

Root

A process that allows users of cell phones and other devices running the Android operating system to attain privileged control (known as "root access") within Android's Linux subsystem, similar to jailbreaking on Apple devices running the iOS operating system, overcoming limitations that the carriers and manufacturers put on such devices.

S

Selective extraction

Performs fast and focused extractions. Pick and choose the applications in which you suspect contains relevant data or leads, and perform a Selective extraction rather waiting several hours for a full file system extraction.

Smart ADB

This method is designed for Android devices that include the "November 2016" security patch. It is supported by OTG compatible devices with OS versions 6.0 and above. Only security unlocked devices are supported.

Smart location

Trusted locations leave the device unlocked for up to four hours when it is turned on, and the device is connected to a secured Wi-Fi access point, trusted Bluetooth device, trusted NFC tag, or if the device detects body movement.

T

TAC

The Type Allocation Code (TAC) is the initial eight-digit portion of the 15-digit IMEI and 16-digit IMEISV codes used to uniquely identify wireless devices. The Type

Cellebrite

Allocation Code identifies a particular model (and often revision) of wireless telephone for use on a GSM, UMTS or other IMEI-employing wireless network.

U

UFD

Once logical, file system, and physical extractions are complete, UFED generates an extraction file, along with a .UFD (text) file. The .UFD file contains information about the extraction, such as which UFED was used (including its serial number); start time, finish time, and date; and hash information. With iOS physical extractions, the .UFD file also contains decryption keys. For binary images, it may contain some information to aid the decoding process.

UFDR

Universal Forensic Extraction Device Report

UFDX

UFED generates a UFDX file when there are multiple extractions for a device. It contains information about each extraction

UFED

Universal Forensic Extraction Device

UFED CHINEX

The UFED Chinex kit, is the solution to complete a physical extraction, decoding of evidentiary data and passwords from mobile devices manufactured with Chinese chipsets; including MTK and Spectrum.

UFED kit

The UFED kit includes connection cables and tips. These are used to connect mobile devices to UFED.

UFED Memory Card Reader

A multi-format card reader that provides either read-only or read-write access to a variety of flash media cards.

UFED TK

A ruggedized mobile forensic solution, purpose-designed for users to perform extraction on asingle ruggedized platform.

V

Voice lock

The user speaks while unlocking the device, and their voice gains access.

14. Index

Cellebrite